ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians

Technologie de l'information — Guide de la sécurité à l'intention des gestionnaires des installations communes et des responsables des systèmes informatiques d'ISTC

ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians

Industry, Science and Technology Canada
Industrie, Sciences et Technologie Canada

Canada

ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians

FP PU 0023-92-03

FOREWORD

The increasing dependency on computers and telecommunications services throughout Industry, Science and Technology Canada (ISTC) makes it imperative that information holdings be properly safeguarded. This handbook is one in a series of three that provide the information required for everyone working at ISTC to properly safeguard departmental assets.

It is only through your support in recognizing security as an important and individual responsibility that we will continue to adequately safeguard our information. I encourage you to follow the measures set out in this handbook and continue to give serious attention to the security requirements of your work.

H G Rogers

H.G. Rogers
Deputy Minister

ACKNOWLEDGMENT

In writing these handbooks, manuals from the Financial and Program Systems Directorate of the Comptroller's Branch, the Information Management Branch and the Federal Office of Regional Development (Quebec) were used as reference. Also, consultations were held with members of the Informatics Managers' Technical Coordinating Group committee.

Thanks are due to all those who helped develop these handbooks. Particular thanks are owed to the members of the department-wide ad hoc steering committee, which included a representative from SILMAC, and to the Training and Development section of the Human Resources Branch.

TABLE OF CONTENTS

Annexes

1. INTRODUCTION

Purpose and scope

This handbook is addressed to:

- shared-facility managers — managers responsible for shared computer facilities, including local area networks (LANs) and mainframe and minicomputer installations; and
- information system custodians — staff members responsible for security requirements and safeguards for information systems and data.

This handbook describes the Industry, Science and Technology Canada (ISTC) information technology security standards and suggests ways to safeguard the department's information and equipment assets. The standards and guidelines set out below cover most situations staff members are likely to encounter, and apply to all equipment and applications used in ISTC.

Unless otherwise indicated, the text is directed to both shared-facility managers and information system custodians. This does not mean that shared-facility managers and information system custodians should duplicate their work. Duties that this handbook has not specifically assigned to one or the other should be allocated in local procedures.

All ISTC staff **must** learn and comply with information technology security standards. To make it easy to identify mandatory government and department security standards, statements that include standards contain the verb "**must**" set in boldface type just as you see it here. There are many ways to meet security standards, and local managers have the authority to decide what is best for their work sites. Guidelines are recommended approaches to solving security problems, and they are identified in the text by verbs such as "may," "can" and "should."

As it is concerned with information technology security, this handbook includes general security procedures described in the ISTC *Security Policy and Procedures Manual* only where necessary for clarity. This handbook does not replace site-specific security procedures for information systems, which are provided at each workplace.

Good information technology security practices involve certain aspects of records management, which are discussed briefly in this handbook. For more information on records management and for complete procedures, consult the Records Management Division.

If you need more information about the technical aspects of information technology security, you should consult the Informatics Security Coordinator, Information Management Branch. For all other security matters, you may consult the Departmental Security Officer at Headquarters.

This handbook focuses on security aspects of current interest to ISTC. Managers of mainframe computers and minicomputers should also refer to the Interim EDP Security Standards for more comprehensive information on government standards (*see* 18. References).

This handbook is part of a series of three. ISTC has also issued the *ISTC Staff Handbook on Information Technology Security*, a general guide for staff of all levels who use computers, and the *ISTC Handbook on Information Technology Security for Responsibility Centre Managers.* At the back of this handbook, you will find a Glossary and a Consolidated Index to the entire series.

Authorities

This handbook is based on the following sources:

- *Information and Administrative Management – Security,* the Treasury Board manual that comprises the Government Security Policy and the Interim EDP Security Standards;
- Treasury Board security bulletins; and
- the ISTC *Security Policy and Procedures Manual,* which comprises the *Classification and Designation Guide* (November 1991) and ISTC Deputy Minister's Directives, including Directive 102-1 – Informatics Security.

2. SECURITY RESPONSIBILITIES

All staff

As part of their basic duties, all ISTC staff **must** safeguard information and equipment in their custody against misuse, theft and deliberate damage, and take all reasonable precautions against accidental damage.

Responsibility centre manager

The manager of each responsibility centre establishes safeguards for the centre's computer equipment, information systems and all data stored in them, and ensures that all staff follow security procedures. Responsibility centre managers may delegate these tasks to local security administrators, shared-facility managers or information system custodians.

Shared-facility manager

The manager of each shared facility establishes safeguards for a multi-user computing facility, such as a LAN, a mainframe or a minicomputer, and ensures that all staff who have access to the facility follow security procedures. In some work sites, certain duties of the shared-facility manager may be delegated to a local security administrator.

As a shared-facility manager, you have the following general responsibilities. You **must**:

- ensure the physical security of the work site where the facility is located;
- safeguard hardware, systems software and related communications equipment; and
- carry out security measures that responsibility centre managers and information system custodians require or recommend for information systems and records.

Here is a partial list of the specific responsibilities of a shared-facility manager. You **must**:

- prepare:
  - sensitivity statements,
  - threat and risk assessments, and
  - contingency plans; and
- ensure that:
  - all data stored in the facility are safeguarded,
  - access to the facility is controlled,
  - written security procedures, backup and recovery procedures and maintenance procedures for the facility are complete and up-to-date,
  - users of the facility have the required security clearance and are appropriately trained in security procedures and backup and recovery procedures,
  - files, software and computer equipment are scanned for viruses as needed,

  - system logs are properly kept, reviewed and controlled,
  - configuration charts and inventories of hardware and software in the facility are maintained, and
  - all staff comply with copyright requirements of software available through the facility.

Information system custodian

The custodian of each information system establishes safeguards for it and ensures that all staff who use the system and its data follow security procedures. The information system custodian also makes decisions concerning the function, design and operation of a system and its data. Other managers (e.g. a shared-data custodian) may make some of these decisions for data bases and certain aspects of systems. Such delegated managers should adapt the content of this handbook to their situation.

Here is a partial list of the information technology security responsibilities of an information system custodian. You **must**:

- prepare:
  - written security procedures,
  - sensitivity statements,
  - threat and risk assessments, and
  - contingency plans;
- establish backup and recovery procedures; and
- ensure that:
  - security requirements are addressed at each stage of systems development,
  - access to the information system is controlled,
  - users of the system have the required security clearance and are appropriately trained in security procedures,
  - information system documentation is complete and up-to-date,
  - the design of information systems meets departmental policies and standards, and
  - sensitive records are appropriately marked.

In some work sites, certain duties of the information system custodian may be delegated to a local security administrator.

Departmental Security Officer

The Departmental Security Officer is the Director of the Security and Safety Directorate, Administrative Services Branch, at Headquarters in Ottawa. This officer holds specific security responsibilities delegated by the Deputy Minister. They include ensuring that ISTC complies with the Government Security Policy and meets government operational standards. Questions about interpreting and carrying out departmental security policy should be addressed to the Departmental Security Officer.

Informatics Security Coordinator

The Informatics Security Coordinator, a member of the Information Management Branch (IMB) at Headquarters, advises and assists the Departmental Security Officer. The Informatics Security Coordinator has specific responsibilities in the areas of security training, compliance monitoring and advising departmental staff on information technology security. This officer also prepares threat and risk assessments as well as contingency plans for critical corporate information systems running on computers administered by IMB.

Local security administrator

A local manager may assign certain local information technology security functions to a staff member other than a shared-facility manager or an information system custodian. Responsibilities of local security administrators are to be documented. Persons assigned the duties should be trained to carry out the functions.

NOTES

3. PERSONNEL SECURITY

Security clearance and enhanced reliability check

Procedures for security screening are described in the ISTC *Security Policy and Procedures Manual.*

The Departmental Security Officer will conduct security clearances or enhanced reliability checks on all staff – managers, supervisors, indeterminate and temporary employees, students and contractors – who require access to classified or designated information to do their work. This includes LAN administrators, programmers, computer operators and network users.

Before you grant users access to your shared facility or information system, you **must** check their security status, following local procedures.

Segregation of duties

To decrease the risk of security violations and breaches and of damage to data and equipment, no individual should be responsible for all aspects of any critical process. In fact, certain responsibilities should not be combined in one position. Unless your work site is very small or unless computer users work only on standalone microcomputers, you should ensure that individuals hold only one of the following responsibilities at a time:

- equipment operations;
- tape library;
- programming; or
- input and output control.

If staff limitations make it impractical to separate these functions, you **must** establish extra safeguards to accommodate the increased level of risk. You should prevent systems development staff from gaining access to production data.

Security training

You are responsible for briefing all staff on their information technology security responsibilities and departmental information technology security standards. You **must** brief staff:

- when they are hired;
- when they leave the work site permanently;
- when they are assigned new duties; and
- when new informatics security procedures are introduced.

You should also hold periodic security briefings to reinforce and refresh information technology security knowledge.

Relinquishing a position

When term employees or contractors leave, when staff members are promoted or transferred, or when ISTC staff relinquish positions for any reason, you **must**:

- cancel their user identifiers and close their user accounts;
- brief them on their security obligations; and
- remind them that the level of their security clearance may be altered.

You **must** also ensure that they:

- transfer and archive records that require preservation;
- destroy or delete records that are no longer needed;
- return door, cabinet and desk keys;
- return encryption keys;
- return all ISTC computer hardware, software and documentation; and
- cancel passwords.

4. PHYSICAL SECURITY

All staff **must** carry a valid building pass in an ISTC work site. You **must** ensure that staff show it before entering security zones, unless the work site is a very small computer centre where all staff members know each other.

Security zones and operations zones

A security zone is an area of the work site that is closed off or set apart to safeguard critical equipment and sensitive information. Access to security zones is strictly limited to authorized staff whose jobs require it.

Consumable supplies and computer equipment that are not critical to operations can be kept in operations zones, which are normal working areas where access is not restricted. For increased safety in operations zones, you should store valuable equipment and attractive items in locked cabinets or offices. If this is not possible, you should ensure that such assets are permanently attached to furniture with cables or bolts.

If staff members print designated documents on printers in operational areas, shared-facility managers **must** establish procedures to prevent the documents from being read by unauthorized people.

Access to security zones

You **must** ensure that visitors to security zones, including cleaning and maintenance staff, sign in and out, if local procedures require it. You **must** ensure that visitors are escorted at all times. If an unauthorized person is found in a security zone, you may have to escort that person out of the security zone. Shared-facility managers **must** ensure that cleaning and maintenance staff who are not permanently assigned to the security zone are supervised.

Deliberate entry to a security zone by an unauthorized person constitutes a security violation. You **must** document such security incidents and report them to the local manager and the Departmental Security Officer.

Design of computer rooms

Shared-facility managers **must** ensure that safeguards are used correctly in rooms housing LAN servers, mainframes, minicomputers or microcomputers used to process sensitive information or information that has a high integrity or availability requirement. These safeguards may include:

- locating the room where it can be monitored;
- installing interior walls that extend from the true ceiling to the true floor of the room (slab-to-slab construction);
- installing approved doors and locking hardware;
- installing surveillance equipment such as intrusion alarms and motion detectors;

- restricting access to authorized personnel; and
- posting "Security Zone" signs prominently at all entrances to the room.

Environmental control in computer rooms

Shared-facility managers **must** help local managers establish procedures to alert staff about malfunctions and situations that require emergency action. Among the measures that should be considered are:

- sensors to detect:
  - air conditioning system failure,
  - floods,
  - power failure, and
  - fire;
- power conditioning;
- surge protection;
- lightning suppression; and
- emergency power shutdown systems.

Securing the power supply

Shared-facility managers **must** ensure that:

- electrical power services for LANs, telecommunications and other shared systems comply with the Treasury Board publication *Fire Protection Standard for Electronic Data Processing Equipment,* Volume 12: *Personnel Management Manual,* Chapter 12;
- distribution panels for power and communications services located outside the controlled zones are secured in consultation with the Departmental Security Officer;
- electrical power and ground return facilities are checked at least twice a year to see that they meet manufacturers' specifications; and
- all backup power systems are tested at least once a year and the results recorded.

Use of flammable and caustic substances in computer equipment areas

Shared-facility managers **must** ensure that flammable and caustic substances used in cleaning and maintenance in computer equipment areas are:

- authorized for use;
- carried in small quantities; and
- stored in unbreakable, covered containers.

5. INFORMATION SECURITY

Need to know

Access to sensitive information **must not** be given except to people who have the appropriate security clearance and who need the information to do their work. Access to sensitive information is a specific job requirement, not a privilege reflecting rank.

Information and records

When you create a record, you gather information in a readable, machine-readable or decipherable form on paper or such machine-readable media as:

- diskettes;
- tapes;
- fixed and removable hard disks;
- optical disks;
- microfiche and microfilm; and
- video screens.

Classified and designated information

Information is *classified* CONFIDENTIAL, SECRET or TOP SECRET if it concerns the national interest and may be exempt from release to the public under the *Access to Information Act*. This means that if unauthorized release, removal, modification or interruption of specific information would endanger public safety, public trust or international relations, the information is required to be classified. For example, diplomatic correspondence that discusses a technology transfer agreement with a foreign government contains classified information. Cabinet confidences, which may be found in Treasury Board documents, are also classified information.

Information is *designated* PROTECTED if its release, modification or interruption would harm individuals or identifiable groups, but not the national interest. For example, personnel evaluation reports and company proposals submitted during competitive bidding contain designated information. Some designated information – birthdates, for instance – is less sensitive than other types, but it needs enhanced safekeeping because there are legislated restrictions on its use. Other designated information is highly sensitive because its release, modification or interruption would threaten the reputation, commercial competitive position or physical safety of an individual, business or identifiable group.

The ISTC *Classification and Designation Guide* will tell you how to assign the correct security levels to records. Consult your supervisor or the Departmental Security Officer for help. The Informatics Security Coordinator will assist you in selecting appropriate safeguards.

Marking classified and designated records

Classified and designated records **must** be labelled clearly so that everyone who uses them will always be aware of the nature of the information they contain. This **must** be done when the record is created.

If you are creating a record containing classified and designated information, you **must** mark it as follows:

- for SECRET and TOP SECRET paper documents – on the cover and on every page;
- for PROTECTED and CONFIDENTIAL paper documents – on the cover and the first page, and on every page if the pages can be separated easily; and
- for data screens and microforms containing sensitive information of any security level – on every screen or form where the sensitive information is recorded.

Computer records containing sensitive information should be written so that the classification or designation is displayed:

- on screen, when the document is retrieved; and
- automatically on printouts, as appropriate for the security level.

For all sensitive records put on paper or machine-readable media, you **must** ensure that file folders or labels bear one of the following symbolic colours to indicate the security levels:

TOP SECRET	Red border and red X across label or back and front of folder
SECRET	Red
CONFIDENTIAL	Green
PROTECTED	Blue

Staff members who find sensitive records that have not been marked with the correct security level may bring them to you or to a manager to be marked and stored correctly. If you are asked to do this, you **must**:

- label the record correctly; and
- ensure that the record is securely stored.

You may need to consult the custodian or the originator of the record for help.

Safeguard requirements for classified and designated records

The safeguard requirements for classified and designated records are set out in Appendix F of Deputy Minister's Directive 70-1 in the ISTC *Security Policy and Procedures Manual.* You **must** safeguard classified or designated information according to its degree of sensitivity.

The sensitive records handled by most employees contain designated information that is not highly sensitive. Upon finishing or interrupting your work with documents or removable machine-readable media containing such information, you **must** store them in locked cabinets. However, you **must** store classified or highly sensitive designated records in appropriate approved security containers (e.g. a steel filing cabinet with a locking bar and a Sargent & Greenleaf combination lock).

You **must** limit access to classified and designated information systems and data stored in computers to authorized users (*see* 8. Controlling Access to Information Technology Systems). You **must** ensure that users are aware that they **must not** print sensitive documents on printers that are located where unauthorized people can see the printout.

Consult your local manager or the Informatics Security Coordinator if you need help or more information. Your manager will need to consult the Departmental Security Officer prior to processing classified information.

Declassifying and downgrading records

When circumstances change and sensitive records no longer need safekeeping, their originator or a person acting for or assigned by the originator **must** downgrade or declassify them. You should review sensitive records in your custody periodically to ensure that their security levels are kept current and correct.

Disposal of classified and designated waste

You **must** ensure that classified and designated waste that you no longer need are destroyed so that no sensitive information can be recovered by an unauthorized person. In regional work sites, you **must** arrange disposal with regional security representatives. At Headquarters, you **must** make disposal arrangements through the Security and Safety Directorate.

You must submit paper documents, failing machine-readable media such as diskettes and tapes, as well as printer ribbons and carbon paper that have been used to produce sensitive records, for destruction. Shredding, mulching and burning are all good methods for destroying classified and designated waste.

Occasionally, a computer that has been used to process sensitive information has to be converted to other uses. Before a hard disk is used for other purposes, you **must** ensure that sensitive records have been removed from it. Because deletion does not remove information completely from machine-readable media, wiping (*see* Glossary) or overwriting files, completely destroying them, is recommended for this task. If the hard disk is damaged or inoperable, it may be impossible to wipe the disk, and it may be necessary to destroy it. Consult the Informatics Security Coordinator for recommended products and advice.

NOTES

6. ADMINISTERING INFORMATION TECHNOLOGY SECURITY

Security procedures and system documentation

In writing or supervising the writing of procedures for each information system, data base, shared facility or site where computers are used, you **must** address security. Without written security requirements, staff can neither fulfil their responsibilities effectively nor be held accountable for shortcomings.

You may assist the local manager in developing and documenting local security procedures. You **must** ensure that they cover:

- responsibilities;
- reporting of security incidents;
- access controls on computer equipment and data, including security zones, passwords, user identifiers and encryption;
- storage and transmission of records and data;
- virus prevention;
- inventories, logs and other computer-related records;
- preparation of sensitivity statements and threat and risk assessments;
- configuration control;
- integrity control;
- data and software backup;
- change control;
- data archiving;
- libraries;
- safeguarding of sensitive records in emergencies;
- contingency plans;
- maintenance and transferring of control to maintenance personnel;
- equipment shutdown and start-up;
- system failure and recovery; and
- printing and distribution of sensitive documents.

You **must** maintain records of all system users and their privileges.

Shared-facility managers **must** ensure that written procedures are prepared for equipment operation and facility administration, as well as for users.

Information system custodians should prepare information system documentation that covers:

- the technical aspects of system;
- programs;

- instructions for operations; and
- instructions for users.

Data bases may be covered in system documentation or documented separately. In either kind of documentation, information system custodians should cover:

- data descriptions;
- logical models;
- physical models; and
- the relationship between data and the information system or systems.

Inventorying information and equipment assets

Shared-facility managers should maintain an up-to-date inventory that includes such details as:

- title, licence number and version number of all software; and
- make, model and capacity of all hardware.

Shared-facility managers should keep an up-to-date list of:

- information systems running in the shared facility; and
- the names of the information system custodians.

Configuration charts

Shared-facility managers **must** maintain up-to-date charts showing all of the physical elements and links of their systems and facilities.

Sensitivity statements

Sensitivity statements document the value of information assets and the worst effect that compromise of or damage to the information could have on users and department clients. Sensitivity statements are used in the preparation of threat and risk assessments and the selection of safeguards.

Information system custodians **must** prepare sensitivity statements for their information systems. Shared-facility managers **must** prepare sensitivity statements for aspects of their shared facilities not covered in the sensitivity statements prepared by information system custodians.

For specific information and instructions on preparing sensitivity statements, consult the Informatics Security Coordinator. Annex A shows you how to prepare sensitivity statements for small systems.

To keep sensitivity statements current, you **must**:

- review them at least once a year; and
- update them when significant changes are made in the assets they describe.

Copies of completed sensitivity statements (original versions and updates) **must** be given to shared-facility managers, the Informatics Security Coordinator and the Departmental Security Officer.

Threat and risk assessments

A threat and risk assessment:

- explains threats to the information system or shared facility;
- substantiates the degree of safeguard required;
- ranks information systems that share facilities and resources in order of priority;
- identifies weaknesses in existing safeguards;
- consolidates facility or location exposure; and
- presents recommendations for improved security, with resource estimates, in order of priority.

Information system custodians **must** prepare a threat and risk assessment for each information system or group of information systems.

Shared-facility managers **must** prepare consolidated threat and risk assessments for their shared facilities. They may also prepare separate threat and risk assessments for aspects of their shared facilities that are not covered in the threat and risk assessments prepared for information systems.

To keep threat and risk assessments current, you **must**:

- review them at least once per year; and
- update them when they are made obsolete by changes.

You **must** send copies of completed threat and risk assessments (original versions and updates) to shared-facility managers, the Informatics Security Coordinator and the Departmental Security Officer.

Threat and risk assessments for critical corporate information systems and data bases operating in the IMB Mainframe and Minicomputer Support group are prepared by the Informatics Security Coordinator.

Annex B shows you how to prepare threat and risk assessments for small information systems. For further information on preparing threat and risk assessments for small information systems, contact the Informatics Security Coordinator.

NOTES

7. VIRUSES

Basic precautions

There are no practical ways to make a computer immune to viruses but, by ensuring that all staff observe security standards, you can lower the risk almost to zero. You **must** instruct users to systematically run recommended, up-to-date antivirus scanning programs:

- regularly for machine-readable media in their custody;
- before copying and using all incoming diskettes, including diskettes from home computers and new, shrink-wrapped, licensed software;
- before using all files and programs received from outside organizations through communications lines; and
- before using all new equipment as well as after equipment maintenance.

Also, you **must** instruct users:

- on procedures for the safe access of outside systems such as public bulletin boards;
- on when and how to scan files and programs received by electronic mail:
- to run only scanned, virus-free software on ISTC equipment, especially when taking ISTC equipment off-site; and
- to avoid running programs of unknown origin, especially illegal copies of software, on ISTC equipment.

Preferably, public systems should be accessed only from standalone microcomputers, or files and programs should be downloaded only onto diskettes that will be scanned before use.

Frequent backups will permit you to recreate files damaged by undetected viruses (*see* 12. Backup and Contingency Procedures).

You **must** establish procedures to ensure that the staff at your work site send only virus-free machine-readable records off-site.

Consult the Informatics Security Coordinator about antivirus programs and for advice on the safest ways to use modems.

What to do on detecting a virus

If you receive a report that makes you suspect that your information system or shared facility has a virus, you **must**:

- stop all affected operations;
- verify that a virus is causing the problem;
- proceed immediately to remove it; and
- inform your local manager, the Informatics Security Coordinator and the Departmental Security Officer.

Speed is essential; the longer you delay in removing a virus, the longer it has to corrupt your data or to damage your equipment.

When a virus appears, it is very important to track down all infected files and, if possible, identify and notify the person who introduced the virus. If a virus remains in any file, anywhere in your system or on machine-readable media used on your system, it will appear again. If you require technical assistance in confirming the presence of a virus or in removing it, contact the Micro/LAN Support hotline at IMB at (613) 954-2833.

8. CONTROLLING ACCESS TO INFORMATION TECHNOLOGY SYSTEMS

Physical controls for equipment and data

Safeguarding hardware, software and data

The safeguards that limit the risk of deliberate and accidental damage to computers, software and data generally function by limiting access to computers and data.

ISTC uses several methods to achieve this, including:

- limiting access to data stored in multi-user computers to authorized users with user identifiers and passwords;
- requiring each user to have a unique user identifier and private passwords — no group identifiers or shared passwords allowed;
- extending only the privileges that users can prove they need, and requiring users to verify their needs periodically; and
- allowing remote users who communicate by modem to access the system only through secure equipment.

User identifiers

User identifiers (user IDs) are unique codes that you **must** assign to each individual user so the computer can identify them and allow access according to established privileges. You **must** ensure that access control tables indicating user privileges are guarded from unauthorized access or are encrypted.

Passwords

In this handbook — and in general data processing operations — a "password" is a unique character string that a user **must** key in before a system will allow access to specific data or software. It is not the WordPerfect™ "password" feature, which is, in fact, a simple form of encryption.

You **must** ensure that users under your supervision change their passwords:

- at least monthly, if they use TOP SECRET data — otherwise, at least quarterly; and
- if you ask for them to be changed.

As well as following these rules, users can and should change their passwords whenever they think they should.

You **must** direct that passwords:

- are kept private to prevent unauthorized access;

- are not displayed by software that authenticates a user's identification; and
- are cancelled when staff leave the work site permanently.

You **must** direct users under your supervision to select passwords that are:

- random;
- five or more characters long; and
- reasonably hard to deduce.

For example, users can take the last three letters of two different words, or the first four letters of a word and two random digits. Dates or real words, especially names, are too easy to figure out.

Passwords **must never** be recorded in readable format. This means you **must** ensure that users do not:

- record them in a computer, except in encrypted form;
- post them anywhere in sight, especially not on desks or computers (yes, there really are people who do this);
- write them on a slip of paper they keep in their files, briefcase or wallet;
- give them to anyone else;
- embed them in information systems software code; or
- include them in unsecured automatic logon procedures stored in any computer.

In a critical system, you **must** establish procedures for backup users to access data without sharing the regular users' passwords.

When you have to record passwords, here are some suggestions:

- write them on a diskette and store the diskette in a locked cabinet or safe; or
- write them on a piece of paper, seal the paper in an envelope, and store the envelope in a locked cabinet or safe.

Administration of access controls

You **must** establish procedures to ensure that all user IDs and passwords are:

- under central administration and central software control (but users may choose their own passwords); and
- given only to the user concerned, orally or in writing, and not by telephone, fax or electronic mail unless they are encrypted.

When you assign user IDs and passwords, you should:

- have users sign an acknowledgment that they agree to obey the terms and conditions established for your facility or system;

- keep up-to-date user lists and profiles that include level of security clearance, access authorization as well as user ID; and
- get annual written verification that they still require and are authorized to have computer access.

Refer to Annex D for a sample User Introduction Sheet. This form is not intended to replace local written procedures. You could adapt this form for information system users.

Access suspension

It is strongly recommended that you suspend user IDs and passwords automatically after users have passed an established violation threshold – three invalid access attempts, for instance. After the third time a user tries to access files or applications without permission, withdraw computer privileges while you investigate the situation.

Also, you should suspend user IDs and passwords that have not been used for a reasonably long time.

Automatic logoff

As an added security measure, you should program computers to log off terminals automatically when they have been inactive for a predetermined time.

Use of powerful software

You **must** limit access to terminals and software that allow more access privileges than are usually granted to regular users. You may consider locating such terminals in security zones or secure rooms, and training the staff who use them to log off when they leave their workstations.

Storing machine-readable records

Removable machine-readable media

If you have in your custody removable machine-readable media (portable computers, removable hard drives, optical disks, diskettes and tapes) that contain classified or designated records, you **must** ensure that they are marked with the level of the most sensitive information they contain. You **must** store machine-readable media containing sensitive records in the approved security container appropriate for their security level (*see* 5. Information Security, above). Also, you **must** ensure that users store sensitive machine-readable media correctly.

Deletion does not remove information completely from machine-readable media. You **must** ensure that sensitive records are wiped or overwritten, or that malfunctioning machine-readable media are destroyed (*see* 5. Information Security, above).

Removable machine-readable media containing unclassified and undesignated information do not have special storage requirements, but the information is a valuable asset that you should safeguard against corruption and such hazards as fire and vandalism.

Fixed hard disks

You **must not** store classified and highly sensitive designated information on a fixed hard disk, even if it is in a standalone microcomputer kept in a security zone. Keep it on diskette (or other removable machine-readable media) and store it in an approved security container (*see* 5. Information Security, above). Even unclassified and undesignated information stored on fixed hard disks in computers that are not in security zones may need special protection to maintain integrity and availability.

Computer hardware and software controls may be used, but certain basic access controls can be by-passed fairly easily by a determined person. Computer locks and password protections can be overcome; a hard disk can even be removed from the machine. If you have in your custody computers that do not have adequate safeguards, you **must** ensure that sensitive records stored in them are destroyed by wiping or overwriting.

Encryption using a convenient commercially available package recommended by the Informatics Security Coordinator may be an adequate safeguard. You **must** make sure that procedures allow access by an authorized backup person.

Certain software packages, including WordPerfect™, can back up files automatically. This is usually done in one of two ways:

- by original backup, which stores the backed up files in the computer under a new name; and
- by timed backup, which deletes the backed up files automatically when the user exits the program.

When such a product is used to process sensitive information on your system, and if the program does not encrypt records as they are created, you **must** ensure that:

- users direct the automatic backup to diskettes; and
- they remove such diskettes and store them in approved security containers.

If the product does not include encryption and if the backup cannot be redirected, you **must** disable the automatic backup feature or have users do it for themselves. Then you **must** direct users to:

- save their sensitive records periodically on diskettes; and
- store their backup diskettes in approved security containers.

Deletion will not safeguard sensitive information that has been saved on a hard disk. Consult the Informatics Security Coordinator for information about programs that destroy files completely by wiping or overwriting them (*see* 5. Information Security, above).

Portable computers are especially vulnerable because they are very attractive and easy to take. Once a computer is stolen, the thief has the leisure to figure out how to modify its hardware and software to get at the data. You **must never** leave portable computers unattended where they can be stolen. You **must** apply the safeguards for hard disks to portable computers with hard disks.

Original software

If it is possible to make a legal copy of original software (*see* 13. Copyright, below), you **must not** use the original software in regular operations. If possible, you **must** secure original software (off-the-shelf or custom-written) to prevent damage and unauthorized modification.

Communications security and computer security

Communications equipment and lines that transmit sensitive data require the same level of safeguard as the computers that process the same data. You **must** apply safeguards recommended in threat and risk assessments; you could, for instance, consider installing integrity controls to ensure that any corruption of or tampering with data can be detected (*see* also 9. Maintaining Hardware and Software, below).

You should also consider installing backup communications equipment and alternative links in case of major system failure or disaster.

Transmitting sensitive information

You should prevent access to sensitive records in communications equipment and lines. Common telephone lines offer little protection for sensitive information because telephone calls can be intercepted in many different ways. Dedicated telephone lines are preferred for communicating sensitive information. You **must** install encryption or some other safeguard approved by the Departmental Security Officer for the transmission of classified and highly sensitive designated information, unless a threat and risk assessment indicates otherwise.

Consult the Informatics Security Coordinator about installing telecommunications safeguards at your work site.

TEMPEST

TEMPEST-compliant communications and data processing equipment is built so that it cannot release information in electromagnetic emissions that can be intercepted by an unauthorized person. ("Tempest" was a code name for the technology when it was being developed.) Normally, for equipment that is not in a shielded room – that is, a room built to prevent electromagnetic emissions – you **must** ensure it is TEMPEST-compliant if you use it to key, store, process, transmit, display or print classified information.

There may be circumstances in which TEMPEST-compliant equipment is not necessary for handling classified information, but the Departmental Security Officer **must** give approval before you do so.

Most designated information does not have to be processed on TEMPEST-compliant equipment. However, you **must** apply this safeguard when processing certain highly sensitive designated information if you have consulted the Departmental Security Officer and a threat and risk assessment indicates the necessity.

You **must** coordinate the acquisition, location, and maintenance of TEMPEST-compliant equipment with the Departmental Security Officer.

Encryption

Encryption is the transformation of digital data in plain text to an unintelligible jumble by a reversible coding process based on a key known only to people who are authorized to see the data.

Encryption is one way to safeguard sensitive data during processing and transmission, and while in storage. There are several off-the-shelf encryption applications varying in the degree of safeguard they provide. For both classified and designated data, you **must** use encryption products that have been approved by the Departmental Security Officer.

The WordPerfect™ password feature is a simple form of encryption – the password is the key. It is easily by-passed and is inadequate to safeguard classified and designated information.

Downloading and uploading files

You **must** ensure that all staff observe the security requirements of all data they download and upload. Also, you **must** ensure that:

- the receiving computer and the communication method they use meet those security requirements; and
- the receiving person has the authorization and security clearance to receive such data.

Dial-up lines

A dial-up line is the easiest route into a computer system for intruders. You **must** safeguard computers equipped with dial-up lines by establishing procedures to verify the identity of anyone accessing an ISTC computer in this way.

You **must** establish different access controls:

- for recorded users who hold ISTC user IDs and passwords; and
- for access by the general public.

Possible controls include:

- voice verification – establishing computer access only on request through a voice telephone;
- callback modems – using a modem that will not allow access to callers for whom it has no predetermined callback number;
- password control – stringent password authentication for callers accessing the modem; and
- segregation – allowing modem access only to separate equipment, such as a standalone microcomputer.

NOTES

9. MAINTAINING HARDWARE AND SYSTEMS SOFTWARE

Authorization

Shared-facility managers **must** authorize all maintenance of hardware and systems software before it is performed. The Departmental Security Officer **must** authorize all maintenance of TEMPEST-compliant equipment.

On-site maintenance

All maintenance staff **must** hold security clearance equal to the security level of sensitive records processed by and stored in the computer.

You **must** ensure that maintenance staff working on-site are escorted whenever they are working with critical equipment. You should remove all sensitive data from hard disks before maintenance staff come in to work on equipment used to process sensitive data. If this is not possible, you **must** take steps to ensure that sensitive information is not accessed, copied or modified. For example, you may have to assign an escort to supervise maintenance staff.

You **must** disable communications links that are used for maintenance until they are needed. You **must not** allow them to be used except under close supervision.

After maintenance, you should scan the equipment for viruses.

Off-site maintenance

When you send equipment off-site for maintenance, you **must** ensure that all sensitive data are copied to diskettes and wiped from hard disks or overwritten.

When equipment is returned to your custody from off-site maintenance, you **must**:

- check that only the authorized maintenance work has been done;
- check the equipment rigorously to ensure its security features have not been by-passed, damaged or compromised; and
- scan the equipment for viruses.

Testing equipment and systems software and recording results

After maintenance work is done, you **must** test systems to ensure that they work properly. It is not unusual for new hardware or software to produce unwanted side effects or incompatibilities with other components. You should develop standard tests, including scans for viruses, for representative features of your shared facility. You should run the standard test periodically.

You **must**:

- develop a comprehensive set of test data to detect changes in your shared facility; and
- keep records of all maintenance and of your test results.

When changes are made to systems software, you **must**:

- develop specific criteria to test the change;
- test all changes to systems software thoroughly; and
- document the test results for future reference.

Program library changes

Shared-facility managers **must**:

- restrict access to program libraries; and
- ensure that changes are correctly documented.

10. CARE OF COMPUTERS AND MACHINE-READABLE MEDIA

Care and cleanliness

Computer equipment is vulnerable to heat, dust, liquids, power surges, magnets and many other influences.

Shared-facility managers are responsible for the care of computers. That responsibility includes ensuring that staff take care of the equipment they use.

Here are some directions and suggestions for keeping computers clean and safe.

You **must** ensure that:

- all magnetic media (diskettes, tapes and hard disks) are protected from magnets and electronic devices that contain magnets or generate magnetic fields, such as speakers and certain telephones;
- diskettes are not left lying around without their protective jackets;
- no one bends diskettes or uses staples or paper clips on them;
- no one touches the shiny surface of a diskette; and
- no one writes on a diskette with a sharp instrument.

You should ensure that:

- write-protect tabs are used on read-only diskettes to prevent damage to files;
- papers and other items are kept clear of the air vents in equipment to prevent overheating;
- food and liquids are kept away from computers and machine-readable media;
- computer equipment is covered or packed up when it is not being used, when it is being moved, and when the environment is very dusty, such as during renovations; and
- manufacturers' preventive maintenance instructions are followed.

NOTES

11. MONITORING COMPLIANCE

All staff are responsible, to some extent, for monitoring compliance with controls that are under their authority.

Inspections

Shared-facility managers **must** conduct security inspections of the facilities they control at least once a year. They **must** record the inspectors' names, their findings and specific recommendations and send copies of the recommendations to the Informatics Security Coordinator and the Departmental Security Officer.

Aspects that should be reviewed include:

- written procedures;
- sensitivity statements and threat and risk assessments;
- contingency plans;
- records of users;
- control records of remote users;
- computer access logs and records review logs;
- integrity controls;
- inventory logs;
- backup records;
- maintenance records;
- change control records;
- software licences;
- security markings of documents and machine-readable media;
- storage of sensitive documents, equipment and machine-readable media; and
- location of terminals.

The Informatics Security Coordinator may conduct or direct managers to conduct additional inspections of information technology security.

The Royal Canadian Mounted Police Security Evaluation and Inspection Team (RCMP SEIT) will examine on-site security measures on request and make recommendations. The Departmental Security Officer coordinates SEIT inspections.

Audits

The Operations Audit Branch of ISTC and the Office of the Auditor General of Canada conduct periodic audits of information technology security. A typical audit will cover:

- whether security procedures are documented and available to staff;

- whether staff have been taught government and department policies and are trained in procedures; and
- whether staff follow procedures.

Auditors will:

- compare local conditions with government and departmental policies and standards;
- check local written procedures; and
- check audit trails to track user activity and data transactions.

Audit trails are records that allow staff, supervisors and auditors to review all transactions and significant actions. They are necessary because they:

- enable staff to analyze problems and come up with solutions;
- identify who was responsible for an action; and
- provide documentary evidence for disciplinary or legal proceedings.

Security records

All computer systems need periodic maintenance of hardware and software. When a problem appears, someone has to find out when it started, what caused it and how to fix it. Also, upgrades to hardware and software have to be planned. Therefore, someone has to be able to find out what the computer has done and when.

Depending on the importance and size of the system, therefore, managers will direct staff to keep records on some or all of these activities:

- updates of hardware and software;
- changes in configuration;
- problems and solutions;
- changes to any components in the facility;
- arrival and departure of visitors;
- activities outside normal working hours;
- computer operations (console logs);
- logons, file accesses and user ID and password changes (security logs);
- failed access attempts;
- system jobs or steps (system logs);
- utilities maintenance;
- testing; and
- changes to computer-access privileges.

Data archiving and retention schedules

Records accumulate, filling storage space and causing computers to slow down. You should, therefore, periodically purge your files of older records. You **must**, however, handle purged records in accordance with departmental records management requirements – consult your nearest Records Office for help or more information.

Consult the Informatics Security Coordinator for information on secure off-site storage for all types of machine-readable media.

You should establish retention schedules for security logs so they are available for periodic security inspections and audits and are disposed of when they are no longer needed. You **must** keep logs for at least three months, but it would be better to keep them for six months to a year. The retention period for logs of archival value is considerably longer. Consult the nearest Records Office for specific information about retention schedules.

You **must** analyze all available logs regularly, including logs of invalid access attempts. Local managers will assign analysis and filing functions. You can copy large logs to a computer file for on-line analysis.

Security incident procedures

The disappearance of documents and diskettes, and unusual events such as unaccountable changes to software and data, are potentially serious security incidents. Incidents that look trivial when considered in isolation can look quite different when considered with other incidents in the work site or in the building.

Working with the local manager, shared-facility managers **must** develop procedures for all staff to follow in reporting security incidents. These procedures should:

- define a security incident;
- state how to report a security incident;
- state who has what responsibility for action; and
- list what records to keep.

The local manager will appoint a staff member to record security incidents and report them to the Departmental Security Officer.

Refer to Deputy Minister's Directive 78-1 in your copy of the ISTC *Security Policy and Procedures Manual* for the complete policy on security incidents and how to report them.

NOTES

12. BACKUP AND CONTINGENCY PROCEDURES

Daily backup

Backup is one of the most important security measures. You **must** establish a schedule of regular backups for each information system and shared facility. Shared-facility managers **must** inform all users of the backup schedule.

Users with special processing requirements will consult shared-facility managers to establish backup schedules that meet their needs. Here are some alternative types of backups:

- incremental backup, which backs up only the files changed since the last full or incremental backup;
- differential backup, which backs up all the files changed since the last full backup;
- full backup, which backs up all files on the system; and
- selective backup, which can be any of the above types of backup, including or excluding specific files.

It is extremely important to ensure that users and operators are taught how to check that they have completed their backup procedures successfully. Otherwise, backup files could be unusable because of some processing error.

Storing data and software backups

Shared-facility managers **must** ensure that backup media are stored in a safe place away from active files. This prevents loss of both the latest backup and active files in the same incident. If the data being processed are critical to recovery and operations, or if they would be very difficult to replace should there be a disaster, shared-facility managers **must** ensure that backups are stored off-site. In some locations, the National Archives of Canada picks up, stores and delivers records free of charge. The Informatics Security Coordinator will help you arrange secure off-site storage for all machine-readable media.

You **must** ensure that the location of stored backup data and software is recorded accurately. You should also ensure that encryption keys and passwords required to access the data are recorded according to the precautions for passwords and key material (*see* 8. Controlling Access to Information Technology Systems, above).

Shared-facility managers **must** ensure that enough generations of backup data are kept to permit recovery of uncorrupted data. Think about how long an error or malfunction can remain undetected in a system. It is sometimes necessary to reprocess old data when a system has had a long-standing problem. If backups are destroyed prematurely, there will be no valid data to work with.

Recovery

Shared-facility managers **must** test data recovery procedures periodically, and always after modifications to related hardware and software. Data can be lost despite regular backups if a routine software update makes the backup data incompatible with the system.

Uninterruptible power supply

Equipment is available for continuing to supply power to a computer for a limited time after a power failure. This equipment allows time to back up data and shut down equipment. Shared-facility managers should consider installing uninterruptible power supply equipment if threat and risks assessments recommend them.

Backup staff

You should keep an updated list of your backup staff on hand and ensure that they are trained.

Contingency plans

Contingency plans describe the arrangements made and steps to be taken to minimize the impact of the loss of the usual computer facilities or resources. The arrangements may provide for reduced services by the affected system, full service by a backup system or service with no computer resources at all.

The manager or custodian in charge **must** prepare contingency plans for each shared facility and information system, according to the following distribution of responsibilities:

- information system custodians are responsible for the preparation of contingency plans for the information systems in their custody;
- other managers who share information system custodians' duties are responsible for contingency plans for the aspects under their authority (for example, shared-data custodians are responsible for the preparation of contingency plans for the shared-data structures in their custody that are considered to be outside information systems);
- shared-facility managers are responsible for the preparation of contingency plans for the facilities they manage;
- IMB is responsible for the preparation of contingency plans for equipment and software under IMB authority; and
- managers with standalone microcomputers in their custody are responsible for the preparation of a contingency plan covering their equipment and records.

Here is a partial list of your basic contingency planning responsibilities:

- preparing procedures for safeguarding sensitive records and equipment in an emergency;
- preparing procedures for continuing service with backup resources or alternative arrangements; and
- training staff in their responsibilities under the contingency plan.

You **must**:

- prepare contingency plans for all new systems before they are implemented;
- test contingency plans at least once per year;
- review contingency plans at least once per year; and
- update contingency plans each time recovery requirements or hardware and software are changed.

When contingency plans are prepared and updated, you **must** send copies to the local manager, the Departmental Security Officer and the Informatics Security Coordinator.

Annex C explains the contents of a basic contingency plan.

NOTES

13. COPYRIGHT

Canadian copyright law

Canadian copyright law restricts the use of purchased software. When you buy software legally, it comes with a licence that states how you are permitted to use it; usually, you are permitted to install it or use it on only one computer at a time and to make a backup copy.

Anyone who copies licensed software for an unlicensed user has breached the *Copyright Act* and is liable under the *Criminal Code of Canada.*

Responsibilities

ISTC complies with copyright legislation without exception. You **must** ensure that:

- only legal licensed software is used by the information systems in your charge; and
- software is made available through the shared facilities only in accordance with the terms of the licence.

When you grant computer privileges to new users, you should have them sign an undertaking:

- to copy software and proprietary documentation only as authorized under the licence; and
- not to use any software at ISTC in violation of its copyright agreements.

NOTES

14. INTEGRITY CONTROLS

Types of integrity controls

To protect your data from corruption and unauthorized manipulation, you **must** build integrity controls into your information system:

- to ensure that the results of its processes are correct and complete; and
- to prevent and detect deliberate or accidental unauthorized data modifications.

You should also consider integrity controls for computer processes other than information systems (e.g. spreadsheets).

Integrity controls **must** be appropriate to the value of the information systems they safeguard. Typical integrity controls are checks built into the information-processing system, such as:

- reconciliations of input and output;
- data matching with other sources;
- input authorization checks; and
- edit checks.

Other types of integrity controls are:

- access control;
- separation of duties; and
- regular comparison of programs on your system with original software or with reliable backup copies.

NOTES

15. PLANNING

Yearly planning cycle

You **must** organize information technology security improvements in a yearly planning cycle. In your planning, you should cover:

- completing and updating sensitivity statements and threat and risk assessments;
- contingency planning;
- conducting security inspections;
- testing safeguards and security procedures; and
- establishing new safeguards and security procedures.

Whenever you contemplate changing your systems and facilities, you **must** assess their impact on your security measures and plan appropriate changes to your safeguards.

NOTES

16. SYSTEMS DEVELOPMENT AND MAINTENANCE

Planning safeguards for information systems

Information system custodians **must**:

- include security controls for their systems in every development phase, especially during system design;
- ensure that, when designing large systems, sensitivity statements and threat and risk assessments are prepared at the start of development and updated in later phases;
- review security requirements and compliance with security policy and guidelines during each phase of large system development; and
- ensure that, when designing small systems, sensitivity statements and threat and risk assessments are prepared at the start of development and updated if necessary at the end of development.

ISTC develops large and small information systems in different ways. A project initiation proposal (PIP) may be necessary, which should specify the security level of the information to be processed. You should consult the IMB liaison officer.

Change control for information systems

Information system custodians **must** establish a rigorous procedure to check that:

- changes are approved;
- changes to information systems software have been done correctly and tested;
- no extraneous codes have been added; and
- no security codes have been removed or inhibited.

You **must** document all changes by recording:

- the name of the information system or shared facility;
- the date changes were made;
- a description of the intended change;
- the reasons for the change;
- a description of the changes actually made; and
- the names and signatures of the staff who:
  - requested the change,
  - approved the request,
  - made the change, and
  - tested the change.

When a change justifies it, you **must** update sensitivity statements, threat and risk assessments, and contingency plans.

Testing information systems

New systems should be tested thoroughly prior to implementation. In addition, after maintenance work is done, you **must** ensure that systems are tested and work properly. It is not unusual for a change to produce unwanted side effects. You should test the specific changes and also run standard comprehensive tests of representative features.

17. CONTRACTING FOR SERVICES AND SUPPLIES

Choosing appropriate safeguards

When you prepare a contract, you **must** specify:

- the federal and departmental security standards that the contractor is required to meet;
- the security clearance or reliability screening levels required for all contract personnel;
- the security level of the information to be processed; and
- the security requirements of the goods or services to be supplied.

When necessary, you should include in the contract a requirement that the contractor return all data and software to ISTC on the delivery date.

You should require suppliers of software to:

- certify that the software does only what it is intended to do and nothing else;
- certify that all the functions of the software are described in the documentation; and
- provide a comprehensive guarantee that the software does not contain any malicious code.

Dependency on suppliers

Excessive dependency on one supplier increases risks. To limit this risk, you can:

- use common, commercially available hardware and software; and
- ensure that all products received from a supplier are documented well enough to permit maintenance and support by a different supplier if needed.

NOTES

18. RESOURCES

References

The ISTC *Security Policy and Procedures Manual,* which comprises the *Classification and Designation Guide* and the Deputy Minister's Directives, is issued to all staff when they begin work with the department. You can get additional copies from the Security and Safety Directorate and it is available in the departmental library.

Information and Administrative Management – Security, better known as the Government Security Policy (actually the title of one of its sections), is a Treasury Board manual. It also contains the Interim EDP Security Standards (GES/NGI-14). This is also available from the Departmental Security Officer or the departmental library. A draft of a new version of the Interim EDP Security Standards is included in two manuals that are available from the Informatics Security Coordinator: *Technical Security Standards for Information Technology* and *Small System Security Guidelines.*

There are two other guides in this series: *ISTC Staff Handbook on Information Technology Security* and *ISTC Handbook on Information Technology Security for Responsibility Centre Managers.* Both handbooks are available from the Departmental Security Officer or the departmental library. Both this guide and the one for responsibility centre managers include a Consolidated Index to the entire series.

Resource personnel

If you have questions about information technology security, consult:

- your colleagues – other shared-facility managers and information system custodians;
- the Informatics Security Coordinator; and
- the Departmental Security Officer.

NOTES

ANNEXES

A. SENSITIVITY STATEMENT FOR SMALL SYSTEMS

Sensitivity statements document the value of information assets and the worst-case impact to users and departmental clients should the system be compromised, in error, or disrupted. They are prepared for all information systems and for all shared computing facilities. They may also be prepared for shared data not included in the sensitivity statements for information systems.

Large information systems require a full sensitivity statement. Advice on how to prepare them is available from the Informatics Security Coordinator. This annex provides instructions on how to prepare sensitivity statements for small systems, which may include information systems, office support software, shared facilities and shared data. The instructions should be interpreted as appropriate for each type of system. For information on who prepares the sensitivity statements and how they are used, *see* 6. Administering Information Technology Security, in the body of this handbook.

Once the sensitivity statement (original and updates) is complete and signed, it is to be delivered to the Informatics Security Coordinator, Information Management Branch (IMB), and to the Departmental Security Officer. Sensitivity statements prepared for information systems or data bases hosted in shared computer facilities should be delivered to the manager of the shared facility.

A WordPerfect™ file version of this annex is also available upon request from the Informatics Security Coordinator. You can use it to complete a sensitivity statement electronically. Make a backup copy of the file before you start just in case you need to restart. Then, place the cursor at the desired position and key the appropriate information. Please do not use the "typeover" mode to answer the questions because you may alter the form and lose some of the questions. If you have any questions or need assistance, please contact the Informatics Security Coordinator.

This document will be deemed PROTECTED information once completed.

Date □ New Statement □ Revised Statement

Small System Description Section

1. Full name of small system (information systems/shared facility/shared data) addressed by the sensitivity statement (note that this name will be used for updating the ISTC departmental inventory of systems held in the ISTC data dictionary, when applicable).

2. Description of small system. Describe the main functions of the small system, the type of data processed, who the users are, update or processing frequency, linkages to other applications, systems and services. For applications, explain if different versions are used in different equipment. Current charts of software components with their interrelationships should be attached.

3. Describe the materiality of the small system (if more than one equipment type is used, you may wish to relate your entries to the type):

   Equipment used:

   Software brand used (data base, compilers, operating system, other):

   Communications links used:

   Number of main records held:

   Number of transactions processed:

   Number of persons using information system/service:

   Dollars processed:

4. Provide the name of the organizational unit within ISTC that has custodial responsibility for the system. Also, provide the sector and region or indicate Headquarters.

5. Provide the name and title of the individual designated as the small system custodian by the custodial organization.

   Name: Title:

   Tel.: E-mail name: Fax:

Confidentiality Requirements

Confidentiality pertains to the impact on the Department of accidental or deliberate disclosure, removal or theft of data and software. Such data and software should have a security classification/designation according to government policy (TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED and undesignated).

6. Identify the highest security classification/designation of any of the data. The security requirements involved in answering this question are presented in the *ISTC Classification and Designation Guide.*

   □ TOP SECRET □ SECRET □ CONFIDENTIAL □ PROTECTED □ undesignated

7. Give reason for security level. Also, describe the nature of loss or damage that would occur if data were compromised.

[The ISTC *Classification and Designation Guide* describes the reasons for the security level (for example, for PROTECTED information the reasons are: law enforcement and investigations; safety of individuals; competitive position of government; government research; undue benefit to a person; third-party business information; testing procedures, tests and audits; solicitor-client privilege; information obtained in confidence from other governments; medical records; and advice, personal information and statutory provisions).

Examples of possible damages are: embarrassment to the Minister; non-compliance with legislation; financial costs: loss of confidence in the department; damage to individuals, corporations, or other organizations; and jeopardizing of evidence in prosecutions.]

Availability Requirements

Availability relates to need for uninterrupted availability of the small system.

8. What is the maximum period that can be tolerated should the small system become unavailable?

Number of	Hours	Days	Weeks	Months

9. Why? What is the impact if small system is not available?

[This may identify the impact in such terms as the ability to perform the function, data currency/integrity, the cost of alternative procedures, inability to meet ongoing government commitments, delays in service to the public, inability to meet statutory requirements, and costs of idle personnel. The criticality of the system or service may rise with the amount of downtime and it may vary with the time of the year when it occurs (e.g. fiscal year end). Also, the impact may be on a linkage between the system and other systems.]

Integrity Requirements

Integrity refers to the prevention of corruption or modification of information, whether accidental or deliberate.

10. What is the requirement for data accuracy?

[This is best expressed as the acceptable error rate when possible. For example, you may say that information needs to have an overall error rate of less than 0.4% (or 1 in 250) with certain data elements having an error rate of less than 0.01% (1 in 10 000). The numbers of actual errors experienced in the system could be used as a reference. Otherwise, integrity requirements may be expressed in other manners.]

11. Why? What is the impact if information or processes are not accurate?

[Examples of the need for data integrity are: faulty information leading to wrong decisions affecting the use of *X* resources; inaccurate calculation of payment amounts in the order of *X* dollars; budgets exceeded; embarrassment to the Minister; loss of public confidence in ISTC; wasted time of employees working with erroneous information; and extra work by staff to correct errors.]

Completed by:	Signature:		Tel.:
Sector:	Directorate:	Division:	Section:
Responsibility Centre Manager:	Signature:		Date:

B. THREAT AND RISK ASSESSMENT FOR SMALL SYSTEMS

A threat and risk assessment explains the perils from which the information system/facility should be protected; substantiates the degree of protection required; sets priorities for information systems that share facilities/resources; identifies weaknesses in protection; consolidates corporate exposure; and presents recommendations to improve security, with resource estimates, in order of priority.

The threat and risk assessment for the IMB Mainframe and Minicomputer Support group is prepared by the Informatics Security Coordinator. This annex provides instructions on how to prepare threat and risk assessments for small systems, which may include information systems, shared facilities, shared data and groups of microcomputers. Therefore, the instructions should be interpreted as appropriate to each use. Usually, sensitivity statements are separately prepared for information systems and general support software in a computer facility. The sensitivity statements along with the relevant information on threats and security measures in place are used to prepare the threat and risk assessment. Each small system should be covered in a threat and risk assessment. Threat and risk assessments may be separately prepared for certain small systems. In addition, consolidated threat and risk assessments must be prepared for each shared computer facility covering all the software, data and equipment in the facility. For information on who prepares them, when they are prepared and how they are used, *see* 6. Administering Information Technology Security, in the body of this handbook.

In the event that your situation can be addressed by only one sensitivity statement and a corresponding threat and risk assessment, you may staple them together. Thus, you do not need to complete sections 2, 3 (except for the configuration charts), 5, 6, 11, 13, 21 and 22 in the threat and risk assessment. Just make a note to see the sensitivity statement.

Once the threat and risk assessment (original and updates) is complete and signed, it is to be delivered to the Departmental Security Officer and the Informatics Security Coordinator. Also, threat and risk assessments prepared for information systems hosted in shared computer facilities should be delivered to the manager of the shared facility.

A WordPerfect™ file version of this annex is also available upon request from the Informatics Security Coordinator. You can use it to complete a threat and risk assessment electronically. Make a backup copy of the file before you start just in case you need to restart. Then, locate the cursor at the desired position and key the appropriate information. Please do not use the "typeover" mode to answer the questions because you may alter the form and lose some of the questions. If you have any questions or need assistance, please contact the Informatics Security Coordinator.

This document will be deemed PROTECTED information once completed.		
Date	□ New Threat and Risk Assessment	□ Revised

Small Systems Description Section

1. Full name of the grouping of information system(s), facilities, shared data or section hosting microcomputers covered in this threat and risk assessment.

2. List individual information system(s), facilities, and shared data included in this threat and risk assessment. Please use the exact names as they appear in the related sensitivity statements.

Name of information systems/facilities/ shared data	Custodian of small system			
	Name	Title	Tel.	Fax

3. Describe the materiality of the small system. Where applicable, this should summarize and supplement information from the related sensitivity statements:

   Equipment used:

   Software used (data base, compilers, operating system, other):

   Communications links used:

   Number of records held:

   Number of transactions processed:

   Number of persons using information system(s)/service:

   Dollars processed:

   Current configuration charts of the hardware and communications lines should be attached.

4. Name of organizational unit within ISTC that has custodial responsibility for the system. Also, provide the sector and the region or indicate Headquarters.

Confidentiality

Confidentiality pertains to the impact on the department of accidental or deliberate disclosure, removal or theft of data and software. Such data and software should have a security classification/designation in accordance with government policy (TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED and undesignated).

5. Identify the highest level security classification/designation of any of the data to be processed:

   □ TOP SECRET □ SECRET □ CONFIDENTIAL □ PROTECTED □ undesignated

   This should specify the highest level of security indicated in the related sensitivity statements.

6. Give reason for security level. Also, describe the nature of loss or damage that would occur if data were compromised. This should summarize the reasons given in the related sensitivity statements.

7. List potential threats and probability of occurrence (high, medium, low). Probabilities should be indicated without considering the safeguards in place.

Threat	**Probability of occurrence**
Foreign government	
Organized crime	
Media	
Lobby groups	
Special interest groups	
Malicious computer hackers	
Disgruntled employees	
Accidental error	

8. Provide a summary of actual breaches in last three years (indicate whether accidental or deliberate).

9. Identify weaknesses in current safeguards to protect confidentiality (*see* 6. Administering Information Technology Security, in the body of this handbook).

10. Recommend actions to correct weaknesses or improve security measures.

Availability Requirements

Availability relates to need for uninterrupted availability of a small system.

11. What is the maximum period of time that can be tolerated should the small system become unavailable. This should reflect the highest availability demand indicated in the related sensitivity statements.

Number of	Hours	Days	Weeks	Months

12. List systems or functions of systems to be restored, indicating priorities and target times for restitution. Consider that, in disaster situations, whole systems may not need to be restored at once. Also, consider that systems may have different availability requirements depending on the time of the year.

13. What is the impact if the small system is not available? This should summarize the impacts given in the related sensitivity statements.

14. List potential threats and probability of occurrence (high, medium, low).

Threat	**Probability of occurrence**
Foreign government	
Organized crime	
Lobby groups	
Special interest groups	
Malicious computer hackers	
Disgruntled employees	
Accidental error	
Accidental disaster (fire, water, gas, etc.)	

15. List actual stoppages (longer than two days) in last three years (indicate whether accidental or deliberate).

16. Identify weaknesses in current safeguards to protect availability. Refer to the standards contained in the body of this handbook.

Availability Requirements (continued)

17. Is there off-site backup of data, software and documentation?

18. Is there an agreement in writing for the use of alternate equipment/facilities?

19. Is there a contingency plan?

    Date last updated

    Date last tested

20. Recommend actions to correct weaknesses or improve security measures.

Integrity Requirements

Integrity refers to the prevention of corruption or modification of information, whether accidental or deliberate.

21. What is the requirement for information accuracy? This should summarize the requirements given in the related sensitivity statements.

22. Why? What is the impact of inaccuracies? This should summarize the reasons and impacts given in the related sensitivity statements.

23. Describe the main measures in place to ensure information integrity. The measures may be listed for each related system or summarized (*see* 14. Integrity Controls, in the body of this handbook).

24. Describe actual problems with information integrity in the last three years.

25. List weaknesses in current safeguards to control integrity (*see* 14. Integrity Controls, in the body of this handbook).

26. Recommend actions to correct weaknesses or improve security measures.

Completed by:	Signature:		Tel.:
Sector:	Directorate:	Division:	Section:
Responsibility Centre Manager:	Signature:		Date:

C. PREPARATION OF CONTINGENCY PLAN FOR SMALL SYSTEMS

This annex provides an outline for the contents of contingency plans for small systems. The outline provides only for basic contingency aspects. To ensure the appropriateness of your contingency plan, you should have it reviewed by the Informatics Security Coordinator. If you have any questions or need assistance or guidance in the preparation of contingency plans for large information systems and computing facilities, please see the Informatics Security Coordinator.

A contingency plan describes the arrangements made and steps to be taken to minimize the impact of loss of computer facilities or resources or application system. The arrangement may provide for reduced services, full services or alternate manual procedures.

The term "small system" is explained in the Glossary of this handbook. It can be a small information system, a shared facility not managed by IMB, a collection of standalone computer equipment in use in a section, or a shared data base other than the Corporate Database. It can also be a grouping of other small systems.

The scope and depth of contingency measures will vary widely depending on the nature of the small system, its criticality and the availability of alternate resources. When followed, the outline provided in this annex will produce a complete contingency plan. However, the degree of detail and elaboration of contingency measures to be covered for each plan will vary widely. A standalone microcomputer running a single simple information system may have its plan written in two to four pages. A multi-user computer facility will need a more extensive plan. What is important is not so much the extent of the contingency plan but its comprehensiveness in documenting the measures to be followed to minimize impact in case of disaster. Other documentation may be referred to, if readily available, and may not need to be duplicated. However, it should be considered that in case of disaster, the only readily available references may be the copies of the contingency plan kept at home by the members of the contingency team.

To ensure easy updating of the contingency plan, specific names of individuals should be included in Appendix C. Sections 1 to 7 of the contingency plan should refer only to staff positions.

A WordPerfect™ file version of this annex is also available upon request from the Informatics Security Coordinator. It may be used to assist you in preparing a contingency plan for a small system electronically.

1. Introduction

Purpose.

State the purpose of contingency plan. [For example, it describes the arrangements made and steps to be taken to minimize the impact of loss of the *X* small system.]

Scope.

List the information systems, data bases and facilities addressed. The scope may also indicate relevant organizational units.

Date prepared and when last updated.

Record the date of each plan update.

2. Summary of availability requirements (from threat and risk assessments and sensitivity statements).

For each system, provide:

- Names of systems.
- Required maximum downtime.
- Target time for restitution of service.
- Description of service or portion of service to be restored.

Consider that in disaster situations, whole systems may not need to be restored at once. Consider, too, that systems may have different availability requirements depending on the time of the year.

3. Contingency team

Include a list that provides:

- Names of persons with contingency responsibilities.
- Responsibilities of each person.
- Work telephone numbers.
- Home telephone numbers (so they can be reached if the contingency occurs after hours).

4. Types of emergencies addressed in this plan

Describe the types of emergencies to be used in planning recovery activities.

For example:

Type A — Full loss of primary facilities — alternate facilities available in the same building.

Type B — Full loss of primary facilities — no alternate facilities available in the building.

Type C — Partial loss of primary facilities.

Type D — Facilities not lost but access to building not possible.

Type E — Facilities not lost but utilities (electrical power, telephones) not available.

These types are referred to below in 5. Recovery actions. Different actions will apply to different types of emergencies. Simpler plans may use only one or two more general types of emergencies.

5. Recovery actions when emergencies occur

Recovery actions should refer to the types of emergencies identified above in 4. Types of emergencies, as appropriate. Different actions will apply to different types of emergencies.

5.1. Initiation of emergency procedures

Indicate who makes the decisions declaring emergencies, on what basis, and what immediate measures are to be taken. This section should consider and be in harmony with other existing local emergency procedures.

5.2. Notification procedures

During office hours and outside office hours, tell who is to be notified and by whom. Clearly indicate who are the first persons to be notified. Persons to be notified may include:

- Manager of the computer equipment facility.
- Information System Custodians.
- Deputy Floor Fire Emergency Officer.
- Departmental Security Officer.
- Departmental Informatics Security Coordinator.
- Recovery team members.
- Law enforcement agencies.
- Support service suppliers.
- Off-site backup facility contact.
- Component vendors.

5.3. Security measures

Who is to be responsible for security at primary and alternate sites, and during the transfer of information?

Describe special measures, if any, to be adopted during contingency procedures.

5.4. Recovery activities

- Recovery team assembly — Who is to assemble and where?
- Damage assessment — Who will assess damage, and who will be informed?
- Recovery decision — Who will decide where and how to recover? What needs to be considered in making the decision? Who needs to be consulted?
- Recovery procedures
  - Initiation — Describe initial recovery activities.
  - How is the transition to the alternate site/equipment to be effected?
  - Describe activities to restore the service to users, for example:
    - Installation and set-up of equipment — Where is equipment to be obtained and how? Where is equipment to be installed? What suppliers are to be used? What equipment is to be installed? What existing equipment is to be used?
    - Installation of communications services — Where is equipment to be obtained and how? Where is equipment to be installed? What suppliers are to be used? What equipment is to be installed?

- Installation of software – What software is to be installed? What are the steps? Where and how is software to be obtained? What software initialization will be needed?
- Installation of data – What data are to be installed? What are the recovery steps? What further documentation should be consulted?
- Assembly of documentation – What documentation is needed for computer operations and applications users?
- Testing – How are the hardware, software and applications to be tested? Are there any test files or test routines? What are the verification procedures? Who is to approve the results of the tests?
- Organization of staff at new site – Who will be responsible for assigning responsibilities? What training will be provided and by whom?
- Initiation of records – What records need to be kept of the operation at the alternate site or of alternate procedures? These could be briefly listed and reference made to the regular system documentation.
- Initiation of first level of service – What is included in the first level of service provided by the contingency procedures? How is it to be initiated?
- Initiation of additional levels of service – What additional levels of service will be implemented? What conditions have to be met for each level to be implemented? How are they to be initiated?

- Restoration of resources at primary site – Who will work on restoring service at the primary site? What testing needs to be completed? What systems or functions of systems will be given priority?
- Transition back to primary site – Who will effect the transition? What special procedures are required to terminate the operation at the alternate site or the alternate procedures? What steps are necessary for transferring the operation to the original site?

6. Alternate facilities

This section describes the alternate facilities to be used in case of disaster.

What facilities are to be used? What hardware will be available? What communication facilities will be available? What will the systems software be (operating system, other)? Where are they located? What floor space and furniture will be available?

What software and data will be used? Where is the off-site backup copy? How can it be obtained? How current is it?

What documentation will be used? Where is the off-site backup copy? How can it be obtained? How current is it? If it is in computer media, where will it be printed?

What other supplies will be needed (for example, special forms, diskettes, cassettes, tapes, paper, ink cartridges) and how can they be obtained?

7. Plan testing

Who will test the plan? How? How often?

Record the tests conducted and the results in a log.

Appendixes

A List of sensitivity statements and threat and risk assessments related to the plan and their location.

B List of essential staff members (needs to be cleared with Human Resources Branch).

C List of persons to be notified in emergencies (refer to 3 and 5.2 above):

Name of contact person.

Position of contact person.

Work telephone numbers.

Home telephone numbers.

Reason for contact.

D Agreements for alternate facilities.

Keep a copy of correspondence with hardware suppliers, service bureaus or other.

D. SAMPLE *USER INTRODUCTION SHEET* FORM

The form below is applicable to a LAN. It will need minor changes to be applicable to other computer facilities. A WordPerfect™ file version of this annex is also available upon request from the Informatics Security Coordinator.

Sample *User Introduction Sheet* Form

Welcome to the . . . . Branch LAN.

Your LAN Manager is: . . . . Tel.: Location:

Your LAN Administrator is: . . . . Tel.: Location:

Your LAN User ID is . . . .

Your password is for your exclusive use. It is used to verify your User ID, and it should not be used by anyone else. Protect your password as you would your credit or bank card. All activities on the LAN are logged and you are held responsible for all actions initiated under your ID. If someone else requires access to the LAN, direct that person to the LAN administrator. Do not leave your microcomputer unattended while logged on to the LAN.

If you have any questions regarding how to use the LAN or any of the LAN facilities, please see the LAN administrator listed above. If you have any suggestions for improving this service, please submit them in writing to the LAN manager.

Security

All activities on this LAN or microcomputers must conform to government-wide, departmental and branch policies, directives and procedures. The following highlight the key elements of these rules. They are designed to:

- protect against unauthorized disclosure of sensitive information;
- conform with Canadian laws; and
- protect the LAN and all services associated with it from disruption or interruption, or if unavoidable, to minimize the impact of loss of service.

Copyright laws. All copyright laws, without exception, must be adhered to. This means that no programs available through this LAN or on your microcomputer can be copied for use on another microcomputer. It also means that no unauthorized copy of any program can be run on your microcomputer.

Processing of sensitive information. Because of government security regulations, classified Information (CONFIDENTIAL, SECRET or TOP SECRET) cannot be processed on this LAN. In order to process information designated as PROTECTED, you must take special steps to ensure that access to it is controlled. These steps include encryption protection or storing it off the LAN and microcomputer, on a properly marked diskette. For assistance, consult your supervisor, the LAN manager or the Departmental Security Officer. See also Deputy Minister's Directive 70-1 (which is included in the ISTC *Security Policy and Procedures Manual)* and the three handbooks in the series on Information Technology Security.

Passwords. Deputy Minister's Directive 102-1 — Informatics Security requires all computer passwords be changed at intervals no longer than 90 days. It is your responsibility to update your password. Instructions for doing this are available from your LAN manager. Note that this does not apply to the WordPerfect™ "password," which is in fact an encryption key and can remain unchanged for the life of the document.

Passwords to other microcomputers, systems, or networks must not be stored in readable file format on the LAN or your microcomputer. For example, automatic sign-on procedures to other computers that include password information must not be stored!

Backing up data. All of your data files held on the LAN are automatically backed up on a regular basis. See your LAN administrator for frequency of backup and additional information. This means your data can be recovered to the time of the last LAN backup, regardless of accident, power failure, etc. If you require more frequent backup than is supplied by the LAN, you must do the additional backups yourself.

Viruses and virus protection. Computer viruses can be very damaging both to individual computer users and to all other users of an infected LAN. The effort needed to recover from an attack can be long and painful. To minimize the chance of an infection **all diskettes imported into this LAN or used in your microcomputer must first be scanned for the presence of a virus before being processed.** See the LAN administrator for details. If you suspect a virus may have infected your machine, report this **immediately** to the administrator. Speed is essential; the longer reporting is delayed the greater the chance that other data will become infected. Once a virus has been identified it is very important to track down the source and **all** infected files; otherwise it will just reappear at a later date.

Use and protection of your micro facilities. Your microcomputer and supporting software are powerful and valuable work tools. These facilities should be used exclusively in support of ISTC's business operation. The associated hardware and software are often highly valued; they should be afforded protection appropriate to their value.

Changes to your microcomputer. You should inform your LAN administrator of any modifications or upgrades (new cards, modems, memory, etc.) to your microcomputer.

Archiving of files. To release disk space, all files not used or accessed for *nnn* months will automatically be copied to tape and deleted from the file server. If you need to recover them to disk, you will need to see your LAN administrator. Files on tape will be kept for only *nnn* months unless a special request is made to the LAN administrator.

Access to electronic mail. It is possible for other users of the LAN to access your electronic mail unless you invoke its password option. This will require you to enter an additional password every time you access it. This is in addition to the password you need to enter to use the LAN. You should consult your electronic mail documentation.

Please sign below and submit to the LAN manager

Declaration of Acceptance

I have read, understand, and accept the stated conditions that apply to the operation of this LAN.

Signed .... Date ....

User's surname .... Initials ....

Location .... Tel. ....

GLOSSARY

access control methods that control a user's privileges and access to systems, data and capabilities.

audit trail records of transactions that collectively provide documentary evidence of processing; is used to trace original transactions forward to related records and reports or backward from records and reports to source transactions.

authentication the procedure of identifying or verifying the eligibility of a workstation, originator or individual to access specific categories of information; processes that provide protection against fraudulent transmissions by establishing the validity of a transmission, message, workstation or originator.

availability the degree to which a system or resource, such as data, is ready when needed.

classified information information that may be exempt from release to the public under the *Access to Information Act;* information that concerns the defence and maintenance of the social, political and economic stability of Canada and thereby the security of the nation; includes TOP SECRET, SECRET and CONFIDENTIAL information. The ISTC *Security Policy and Procedures Manual* indicates what material is in this category.

COMSEC communications electronic security; the protection resulting from applying cryptographic, transmission and emission security measures to telecommunications, non-telecommunications and information-handling equipment.

confidentiality a term referring to data that must be held in confidence; describes the level of protection that must be provided for such data.

contingency plan a comprehensive, consistent statement of all the actions to be taken before, during and after a disaster (emergency condition), which, if followed, will ensure the required availability of the computers and data resources to maintain the continuity of operations in an emergency.

dedicated line a fixed link from a computer to a specific location.

Departmental Security Officer the Director, Security and Safety Directorate, Administrative Services Branch; has specific security responsibilities delegated by the Deputy Minister.

designated information sensitive information that does not affect the national interest but still requires enhanced safekeeping; PROTECTED information. The ISTC *Security Policy and Procedures Manual* indicates what material is in this category.

dial-up line a link to a computer from any telephone.

download to transfer records from a remote computer to your computer through communications lines.

encryption the transformation of plain data to an unintelligible form through the use of a reversible cryptographic process.

encryption key a unique string of characters that an encryption product uses to encode and decode data.

facility computer equipment; related systems software (operating system, utilities, compilers, data base, security, communications, etc.); media libraries (tapes, diskettes, etc.); on-line libraries; communications equipment; and related supporting equipment (air conditioners, uninterruptible power supply, alarms, etc.).

highly sensitive designated information designated material that requires special safeguards. Refer to the *Classification and Designation Guide* in the ISTC *Security Policy and Procedures Manual* for exact criteria; the advice of the Departmental Security Officer can also be sought.

informatics a generic term covering all information technology equipment, software and services used for the collection, processing, storage, transmission, reproduction and presentation of information.

Informatics Security Coordinator the member of the Information Management Branch (IMB) who advises and assists the Departmental Security Officer; has specific responsibilities for security training, compliance monitoring and advising ISTC staff on information technology security; also prepares threat and risk assessments and contingency plans for critical corporate information systems running in computers administered by IMB.

information system a combination of hardware, software, processes and procedures assembled to accomplish specific business objectives; uses data as input. (This handbook makes a distinction between small and large information systems. The distinction is necessary because they require different types of sensitivity statements and threat assessments. Please seek advice from the Informatics Security Coordinator.)

information system, large an information system that is complex, strategic and corporate in nature (shared by many responsibility centres); is managed by IMB.

information system, small a non-strategic, non-complex information system.

information system custodian the person responsible for the decisions concerning the system's functions, design, operations and data.

information systems software the set of computer programs and other instructions of an information system that handles the specific task to be accomplished by the computer.

integrity a requirement that the information be accurate, complete and dependable; is particularly important for financial systems and decision-support systems.

LAN *see* local area network.

local area network a system of devices interconnected by a continuous medium so that equipment and applications (data or word processors, electronic mail) can operate over a single set of cables; operates within a limited geographic area, usually within a radius of no more than 50 kilometres.

local security administrator a staff member, usually a shared-facility manager or information system custodian, assigned to certain local information technology security duties by the local manager.

logical access control the password administration and other software used to control access to computerized information.

mainframe a large computer, usually simultaneously running several systems and serving many users located at multiple sites.

minicomputer a medium-sized computer that has a smaller processing capacity than a mainframe but is used in the same way.

need to know the principle that only those who require it for their official duties may have access to, knowledge of or possession of sensitive information.

password a unique string of characters used to authenticate an identity; a password is private, unlike a user identifier.

personnel security procedures to ensure that all personnel with access to sensitive information have the necessary authority and clearances.

physical security procedures to locate and design accommodation and establish physical procedures to prevent, detect and respond to unauthorized access; is separate from hardware and software security measures.

policy a statement of intent, desired result or required action; often directs actions to be taken; sets the rules that govern standards, guidelines and procedures.

procedure a document describing specific responsibilities that provides instructions for the completion of tasks at given locations.

record a document or machine-readable medium containing information; any paper, optical disk, or photographic, magnetic or electronic medium in or on which information is preserved in words, pictures, numbers, coded characters or any intelligible, machine-readable or decipherable form.

responsibility centre manager the manager in charge of an ISTC work site, with responsibility for all equipment and information assets and all security measures taken to safeguard them.

retention schedule a schedule that states how long records, such as computer access logs, must be kept, when they should be transferred to the National Archives of Canada, and when they should be destroyed.

scan to use a computer program to search files, machine-readable media or computer equipment for viruses.

secure room a room equipped with an anti-intrusion device and doors with approved locks, located in an area to which access is controlled and limited to very few people.

security container an approved filing cabinet equipped with a locking bar and an approved dial combination padlock, or an approved safe with a dial combination lock. For more precise details, consult the Departmental Security Officer.

sensitive information information that must be safeguarded because its unauthorized disclosure, loss, alteration or destruction would cause perceptible damage to someone or something; must be safeguarded to its level of sensitivity; must be assigned a security level and properly identified; can be classified TOP SECRET, SECRET or CONFIDENTIAL, or designated PROTECTED.

sensitive material a record, information or equipment that is classified or designated or should otherwise not be made available to unauthorized people.

shared-facility manager the person responsible for the hardware, systems software, related communications equipment and data of a multi-user computing facility, such as a mainframe computer, minicomputer or LAN. At some work sites, the security duties of the shared-facility manager are carried out by a local security administrator.

small system may be a small information system, office support software, a LAN, a shared microcomputer, a group of microcomputers, shared data for small information systems or a shared facility not managed by IMB.

software a term used to differentiate computer programs from the metallic circuits (or hardware) of a computer system; a stored set of instructions governing the operation of a computer system.

tampering unauthorized modification that alters the proper functioning of a system or piece of equipment in a manner that degrades the security it provides.

tape library a room or cabinet, to which access is strictly controlled, used to store backup and production copies of data and software; usually comprises both on-site and off-site facilities.

unauthorized person a person to whom access to classified or designated information has not been specifically given.

upload to transfer records from your computer to a remote computer through communications lines.

virus a program inserted into a system for mischievous or malicious purposes; is capable of replicating and attaching itself to other files; may be triggered by a predetermined event or date.

visitor anyone other than site staff.

wiping the procedure of overwriting magnetic media to make previously recorded or deleted information absolutely unreadable and unrecoverable; is used to protect the confidentiality of records.

CONSOLIDATED INDEX

This Consolidated Index includes the key words in all three Handbooks in this series, which are distinguished as follows:

STAFF — *ISTC Staff Handbook on Information Technology Security;*

SFM-ISC — *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians;* and

RCM — *ISTC Handbook on Information Technology Security for Responsibility Centre Managers.*

NOTES

NOTES

NOTES

NOTES

NOTES

COMMENTS

To help us improve these standards and guidelines, we would appreciate your comments. Please tear out this page, fill in your comments and send to the Informatics Security Coordinator, Information Management Branch, ISTC Headquarters.

	Your computer involvement (please check where appropriate)		
	Micro-computer	Mini-computer	Mainframe
User			
Computer facilities manager			
Information system custodian			
Manager overseeing any of the above three			

Name ____________________ Telephone number ____________

Please enter your comments on the other side of this page.

Additional comments

	Please enter **Y** – yes; **N** – no; **N/A** – not applicable			
Handbook section	**Useful?**	**Clear?**	**Sufficient detail?**	**Too much detail?**
Security Responsibilities				
Personnel Security				
Physical Security				
Information Security				
Administering Information Technology Security				
Viruses				
Controlling Access to Information Technology Systems				
Maintaining Hardware and Systems Software				
Care of Computers and Machine-readable Media				
Monitoring Compliance				
Backup and Contingency Procedures				
Copyright				
Integrity Controls				
Planning				
Systems Development and Maintenance				
Contracting for Services and Supplies				

Please explain your comments on the other side of this page.

RECORD OF UPDATES

Date released	Updated by	Notes