ISTC Handbook on Information Technology Security for Responsibility Centre Managers

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

Canada

FP PU 0021-92-03

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
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

1. INTRODUCTION

Purpose and scope

This handbook is addressed to responsibility centre managers in Industry, Science and Technology (ISTC) having direct or indirect responsibility for computer equipment, software, records or information systems. This handbook covers information technology security matters that are your specific responsibility and offers general information on how to carry them out.

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 bold. There are many ways to meet security standards, and you have the authority to decide what is best for your work site. Guidelines are recommended approaches to solving security problems, and they include 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 you **must** provide.

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, consult the Informatics Security Coordinator, Information Management Branch.

On other security matters, consult the Departmental Security Officer.

This handbook is part of a series of three. The *ISTC Staff Handbook on Information Technology Security* is a general guide for staff of all levels who use computers. If you are a responsibility centre manager who is also a computer user, you should use that handbook along with this one. The series also includes the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians*. If you are a responsibility centre manager who is also a shared-facility manager or information system custodian, you should use that handbook along with this one.

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 are responsible for safeguarding information and equipment in their custody against misuse, theft, and deliberate and accidental damage.

All staff are required to follow departmental and local security policies, standards and procedures.

Responsibility centre manager

As manager of a responsibility centre, you have ultimate responsibility for information technology security. You are responsible for establishing suitable safeguards for computers, information systems and data, and for ensuring that all staff follow security procedures in your work site.

You may delegate information technology security tasks to local security administrators, shared-facility managers and information system custodians.

A partial list of your specific responsibilities includes the following duties:

- appointing a manager for each shared facility and a custodian for each information system in your charge;
- assigning each microcomputer (including those used by several individuals) to designated members of your staff;
- ensuring that sensitivity statements, threat and risk assessments as well as contingency procedures are prepared; and
- ensuring that all information technology security violations and breaches are reported to the Departmental Security Officer.

You may also assume any or all of the duties of a shared-facility manager or an information system custodian.

Shared-facility manager

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

A shared-facility manager has the following general responsibilities:

- ensuring the physical security of the work site where the facility is located;
- safeguarding hardware, system software and related communications equipment; and
- applying safeguards for information systems and records that have been required or recommended by responsibility centre managers and information system custodians.

A partial list of the specific responsibilities of a shared-facility manager includes the following duties:

- preparing:
  - sensitivity statements,
  - threat and risk assessments,
  - contingency plans; and
- ensuring 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,
- 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 is responsible for establishing safeguards for it and for ensuring 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. shared-data custodians) may make some of these decisions for data bases and certain system aspects.

A partial list of the information technology security responsibilities of an information system custodian includes the following duties:

- preparing:
  - written security procedures,
  - sensitivity statements,
  - threat and risk assessments, and
  - contingency plans;
- establishing backup and recovery procedures; and

- ensuring 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,
  - information system design 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. 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. You should address questions about interpreting and carrying out departmental security policy to the Departmental Security Officer.

In the regions, all communications with the Departmental Security Officer are usually channelled through the Regional Security Representative.

Informatics Security Coordinator

The Informatics Security Coordinator, Information Management Branch (IMB), advises and assists the Departmental Security Officer. This coordinator has specific responsibilities in the areas of security training, compliance monitoring and advising departmental staff on information technology security. This coordinator 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

You may assign certain local information technology security functions to staff members who are not shared-facility managers or information system custodians. You should ensure that the responsibilities of local security administrators are documented and that persons assigned the duties are trained to carry out the functions.

3. PERSONNEL SECURITY

Security clearance and enhanced reliability check

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

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

You **must** ensure that managers check security clearances for:

- contract personnel before a contract begins;
- new employees before they begin work; and
- staff when they are assigned new duties with different access requirements.

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, individuals should hold only one of the following responsibilities at a time:

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

If staff limitations make it impractical to separate these functions, you **must** ensure that extra safeguards are established to accommodate the increased level of risk.

Security training

You **must** ensure that staff are briefed on their information technology security responsibilities and on departmental information technology security standards:

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

You should also ensure that staff are briefed periodically to reinforce and refresh information technology security knowledge.

You may conduct security briefings yourself or delegate this task to a shared-facility manager, information system custodian or local security administrator.

Relinquishing a position

You **must** ensure that staff members complete routine procedures when they relinquish a position for any reason, such as promotion, transfer, retirement or end of contract or term. These procedures include:

- transferring and archiving records for preservation;
- destroying or deleting records that are no longer needed;
- returning door, cabinet and desk keys;
- returning encryption keys;
- returning all ISTC computer hardware, software and documentation;
- cancelling passwords and user identifiers and closing their user accounts; and

- attending security briefings on their security obligations and changes to their personal security level requirements.

You **must** ensure that employees leaving ISTC permanently also complete the Employee Clearance Record form according to the procedure set out in the ISTC *Security Policy and Procedures Manual.*

4. PHYSICAL SECURITY

Security zones and operations zones

A security zone is an area of the work site that is 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 any computer equipment that is not critical to operations can be kept in operations zones, which are normal working areas to which access is not restricted. For increased safety in operations zones, portable equipment and items attractive to thieves should be stored in locked cabinets or offices.

If printers in operational areas are to be used for designated documents, you **must** ensure that procedures are established to prevent the documents from being read by unauthorized people.

Access to security zones

You **must** ensure that all staff in your work site know that they can be asked at any time to produce a valid building pass.

You **must** ensure that procedures are established for signing visitors in and out of security zones and for escorting them while they are in security zones. Cleaning and maintenance staff not assigned there permanently who have to work in security zones are treated as visitors — signed in and out, and escorted.

Deliberate entry to a security zone by an unauthorized person constitutes, at the least, a security violation. You **must** establish procedures for staff to follow when reporting security violations and breaches to you. You **must** relay all such reports to the Departmental Security Officer.

Computer rooms When you request or allocate space for critical equipment, such as LAN servers, mainframes and minicomputers, or for computers that process classified or highly sensitive designated data, you should choose rooms with walls built from the ceiling slab to the floor slab.

You **must**:

- ensure that computer rooms are equipped with appropriate safeguards;
- ensure that power services for shared facilities and telecommunications equipment comply with Treasury Board standards and are regularly checked; and
- establish procedures to alert computer room staff to equipment malfunctions and situations that require emergency response.

5. INFORMATION SECURITY

Need to know

You **must** ensure that the only people who receive access to sensitive information are those who have the appropriate security clearance and who need the information to do their work.

Information and records

When a record is created, information is gathered in a readable, machine-readable or decipherable form on paper or machine-readable media such as:

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

Classified and designated information

If information is reasonably likely to be exempt from release under the *Access to Information Act* or the *Privacy Act*, and if its unauthorized release, removal, modification or interruption would be against the national interest, it is *classified* CONFIDENTIAL, SECRET or TOP SECRET.

Information is *designated* PROTECTED if its release, modification or interruption is reasonably likely to harm individuals or identifiable groups, but is not against the national interest. Some designated information is very sensitive; 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* explains how to assign the correct security levels to records. Consult the Departmental Security Officer for help. The

Informatics Security Coordinator will assist you in selecting appropriate safeguards.

Marking classified and designated records

You **must** ensure that staff who create classified and designated records label them prominently.

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** ensure that information is safeguarded according to its degree of sensitivity. Highly sensitive information may need to be safeguarded like classified information. Classified information needs very special safeguards. You **must** ensure that the Departmental Security Officer is consulted prior to processing classified information.

You **must**:

- ensure that when staff finish or interrupt their work, they store documents and removable machine-readable media containing sensitive information correctly, putting:
  - designated material in locked containers and
  - classified material in approved security containers; and
- limit access to classified information systems and sensitive data stored in computers strictly to authorized users.

Declassifying and downgrading records

You **must** establish procedures for downgrading or declassifying sensitive records by the originator or a person acting for or assigned by the originator. You should ensure that managers periodically review sensitive records to keep security levels current and correct.

Disposal of classified and designated waste

You **must** ensure that classified and designated waste is destroyed so that no sensitive information can be recovered by an unauthorized person. You **must** also direct staff to submit for destruction all paper documents, faulty machine-readable media such as diskettes and tapes, as well as printer ribbons and carbon paper that have been used to produce sensitive records. In regional work sites, regional security representatives arrange disposal. Headquarters staff arrange disposal with the Security and Safety Directorate.

Computers that have been used to process sensitive information will occasionally have to be transferred to other uses. Before a hard disk can be used for other purposes, you **must** ensure that sensitive records are removed from it. Because deletion does not remove information completely, wiping (see Glossary) or overwriting the information, completely destroying it, 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.

6. ADMINISTERING INFORMATION TECHNOLOGY SECURITY

Security procedures and system documentation

You **must** prepare procedures that address security, or ensure that such procedures are prepared, for each information system, data base, shared facility or site in your charge where computers are used. Unless they have written security requirements, staff can neither fulfil their responsibilities effectively nor be held accountable for shortcomings.

You **must** ensure that local security procedures 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;
- configuration control;
- integrity control;
- data and software backup;
- change control;
- data archiving;
- libraries;
- 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 should ensure that shared-facility managers prepare written procedures for equipment operation and facility administration as well as for users.

You should ensure that information system custodians prepare system documentation that covers:

- the technical aspects of systems;
- the technical aspects of data bases;
- programs;
- instructions for operations; and
- instructions for users.

When data bases are not covered in information system documentation, you should ensure that information system custodians prepare separate documentation that covers:

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

Sensitivity statements

You **must** ensure that a sensitivity statement is prepared for each shared facility and large information system. Small information systems in your charge may be covered in separate or combined sensitivity statements.

Shared-facility managers, information system custodians and shared-data custodians prepare sensitivity statements to document the value of information assets and the worst impact that damage to the information could have on users and department clients. These statements have several uses, including:

- identifying assets for which threat and risk assessments are to be prepared;
- guiding the choice of safeguards; and
- ensuring that management is aware of sensitive processes and assets.

For information on preparing a sensitivity statement for small systems, consult Annex A in the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians.*

You **must** ensure that copies of completed sensitivity statements and annual updates are sent to the Informatics Security Coordinator and the Departmental Security Officer.

Threat and risk assessments

You **must** ensure that all information systems, shared facilities, communication facilities or computers are covered in threat and risk assessments.

The threat and risk assessment:

- identifies vulnerabilities in and threats to the information system and its hardware, software, communications facilities and electronic records;
- describes the extent of safeguards required to eliminate the threats or reduce the risk to acceptable levels; and
- ranks information systems in order of importance for continuation or recovery.

The Informatics Security Coordinator prepares threat and risk assessments for corporate information systems and data bases operating in the IMB Mainframe and Minicomputer Support group. Shared-facility managers, information system custodians and responsibility centre managers prepare other threat and risk assessments.

For information on preparing a threat and risk assessment for small systems, consult Annex B in the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians.*

7. VIRUSES

Basic precautions

There is no practical way to make a computer immune to viruses, but your staff can lower the risk almost to zero if they make frequent backups and use scanning software. You **must** direct staff to use a recommended, up-to-date scanning program:

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

You **must** direct staff using diskettes or programs obtained from outside sources to take the following precautions:

- to use only scanned, virus-free software, especially when using ISTC equipment off-site; and
- never to use programs of unknown origin, especially illegal copies of software, on ISTC equipment.

You **must** direct staff to consult the shared-facility manager before accessing outside systems such as bulletin boards. You should ensure that they access public systems only from a standalone microcomputer. If this is not possible, you **must** ensure that staff download files only onto diskettes, and that they scan the diskettes before using or copying the files.

Also, you **must** ensure that only virus-free diskettes are provided by ISTC to outside organizations.

The Informatics Security Coordinator will advise you on antivirus programs and the safest ways to use modems.

8. CONTROLLING ACCESS TO INFORMATION TECHNOLOGY SYSTEMS

Safeguarding hardware and software

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 identified by user identifiers (user IDs) and passwords;
- requiring each user to have a unique user ID and private passwords – no group identifiers or 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 if they process sensitive data.

User identifiers

User identifiers (user IDs) are unique codes assigned to each individual user so the computer can identify them and allow access according to their established privileges. You **must** ensure that user authentication software does not display user IDs.

Passwords

To help prevent unauthorized access to sensitive data stored in computers, you **must** ensure that:

- users are aware that their passwords are to be kept private;
- authentication software does not display passwords; and

- passwords of staff who have left the work site permanently are cancelled.

Storing machine-readable records

You **must** direct staff who have custody of sensitive records:

- to mark removable machine-readable media with the level of the most sensitive information they contain;
- to store removable machine-readable media containing sensitive records in appropriate approved security containers;
- not to leave classified and highly sensitive designated records on fixed hard disks, even in security zones; and
- to use only encryption software that has been approved by the Departmental Security Officer.

Deletion does not remove information completely from machine-readable media. You **must** ensure that staff wipe or overwrite sensitive records, and destroy faulty machine-readable media.

You **must** ensure that original software is safeguarded against damage and unauthorized modification. If it is possible to copy software legally, you **must** direct staff to use copies in regular operations and not the original.

You should establish procedures to safeguard all records against corruption and such hazards as fire and vandalism.

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** ensure that staff apply the safeguards recommended in threat and risk assessments. You should also consider installing backup communications equipment and alternative links in case of a disaster or major system failure.

Common telephone lines offer little protection for sensitive information because telephone calls can be intercepted in many different ways. Possible safeguards include dedicated lines, encryption, callback modems and voice confirmation. For the transmission of classified and highly sensitive designated information, encryption or some other safeguard approved by the Departmental Security Officer is to be used, unless a threat and risk assessment indicates otherwise.

Information is subject to unauthorized access by interception of electromagnetic emanations. For classified information, you **must** ensure that equipment approved by the Departmental Security Officer (TEMPEST) is installed, unless a threat and risk assessment indicates otherwise and the Departmental Security Officer is consulted.

Most designated information does not have to be processed on TEMPEST-compliant equipment. However, certain highly sensitive designated information may be processed on TEMPEST-compliant equipment if you have consulted the Departmental Security Officer and a threat and risk assessment indicates that it is necessary.

You **must** ensure that the acquisition, location and maintenance of TEMPEST-compliant equipment is coordinated with the Departmental Security Officer.

9. MAINTAINING HARDWARE AND SOFTWARE

Safeguards

You **must** ensure that:

- all maintenance work is authorized by you or a person with delegated authority;
- all maintenance staff working on computers or information systems that process sensitive data have security clearances;
- sensitive data are removed before maintenance or that access to them is prevented during maintenance;
- equipment or information systems are checked and tested after maintenance is completed;
- equipment is checked for viruses after maintenance;
- records are kept of all maintenance; and
- the Departmental Security Officer authorizes all maintenance of TEMPEST-compliant equipment.

When a change justifies it, managers and custodians need to update their sensitivity statements, threat and risk assessments, and contingency plans.

10. MONITORING COMPLIANCE

All staff are responsible, to some extent, for monitoring compliance with controls.

Inspections

You **must** ensure that your shared-facility managers conduct security inspections of the facilities they control at least once per year. You **must** ensure that reports include the inspectors' names, their findings and their specific recommendations and that they are submitted to the Departmental Security Officer.

Depending on the importance of the shared facility or information system, you should review some or all of the following aspects:

- records of users;
- control records of remote users;
- computer access logs and records review logs;
- integrity controls;
- inventory logs;
- backup 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 you to conduct additional inspections of information technology security.

The Royal Canadian Mounted Police Site 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

Operations Audit Branch of ISTC and the Office of the Auditor General of Canada conduct periodic audits of information technology security. 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.

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.

Security logs

When they are available, logs of invalid access attempts **must** be analyzed regularly and kept on file for the inspectors and auditors. You **must** assign analysis and filing tasks.

Archiving records

Records accumulate, filling storage space and causing computers to slow down. You should therefore ensure that your files are periodically purged of older records. You **must** ensure, however, that purged records are archived in accordance with departmental records management retention schedules — consult the nearest Records Office for help or more information.

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 that **must** be reported, recorded and investigated. You **must** ensure that procedures are developed for all staff to follow in reporting security incidents. These procedures should define:

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

You **must** either record security incidents and report them to the Departmental Security Officer yourself, or delegate these tasks to a staff member.

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

11. PLANNING

Planning cycle

Information technology security improvements **must** be organized in a yearly planning cycle. Also, whenever changes to systems and facilities are contemplated, you **must** assess their impact on your security measures and plan appropriate changes to safeguards. Planning 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.

12. BACKUP AND CONTINGENCY PROCEDURES

Daily backup

Backup is one of the most important security measures. You **must** ensure that a regular backup schedule is established for each information system and shared facility, and that all users are informed of the backup schedule.

There are different types of backups that can be chosen. The choice of backup arrangements should depend on:

- how long you can afford to wait until files are recreated; and
- what it would cost to recreate files.

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

Storing data and software backups

You **must** ensure that backup media are stored in a safe place away from active files. This prevents loss of both the latest backup and the active files in the same incident. If the data being processed are critical to recovery and operations, or if they are very difficult to replace should a disaster hit your work site, you **must** ensure that the 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 arrange secure off-site storage for machine-readable media.

You **must** ensure that staff, following the appropriate precautions, accurately record:

- the location of stored backup data and software;
- encryption keys; and
- passwords required to access the data.

You **must** ensure that enough generations of backup data are kept to guarantee that uncorrupted data can be recovered. If a system has had a problem for some time, it may be necessary to reprocess old data. If backups are destroyed prematurely, there will be no valid data to work with.

Recovery

You **must** ensure that data recovery procedures are tested periodically, and always after modifications to related hardware and software. Data can be lost despite regular backups if a software update makes the backup data incompatible with the system.

Uninterruptible power supply

Equipment is available that continues the power supply to a computer for a limited time after a power failure. This equipment allows time to back up data and shut down equipment. You should consider installing uninterruptible power supply equipment if sensitivity statements suggest they are necessary.

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.

You **must** ensure that the manager or custodian in charge prepares contingency plans for each shared facility and information system, as follows:

- information system custodians prepare contingency plans for the information systems in their custody;

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

A partial list of your managers' and custodians' basic contingency planning responsibilities includes the following duties:

- 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** ensure that contingency plans are:

- prepared for all new systems before they are implemented;
- tested at least once per year; and
- reviewed once per year and updated if recovery requirements or hardware and software are changed.

You **must** ensure that copies of original contingency plans and annual updates are sent to the Departmental Security Officer and the Informatics Security Coordinator.

For information about the content of a basic contingency plan, consult Annex C of the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians.*

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 in 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.

Compliance

ISTC complies with copyright legislation without exception. All staff **must** conform to the terms of the licence when copying software. You **must** ensure that software under your jurisdiction is made available to users only in accordance with the terms of the licence.

When staff are granted computer access, you **must** ensure that they sign an agreement:

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

14. INTEGRITY CONTROLS

Types of integrity controls

To protect data from corruption and unauthorized manipulation, you **must** ensure that integrity controls are built into your information systems:

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

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.

You **must** also ensure that staff periodically carry out certain operational precautions, including:

- regularly testing safeguards such as software access controls to ensure that they work properly; and
- comparing the programs running on your system with the original software or with reliable backup copies to ensure that they have not been altered.

15. CONTRACTING FOR SERVICES AND SUPPLIES

Choosing appropriate safeguards

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

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

When necessary, the contract should require the contractor to 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;
- to certify that all the functions of the software are described in the documentation; and
- to 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.

16. 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 Standard (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 handbooks in this series: the *ISTC Staff Handbook on Information Technology Security* and the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians.* Like this handbook, the handbook for shared-facility managers and information system custodians includes a Consolidated Index to the entire series. Both handbooks are available from the Departmental Security Officer or the departmental library.

Resource personnel

If you have questions about information technology security, consult:

- a shared-facility manager;
- an information system custodian;
- the Informatics Security Coordinator, IMB; or
- the Departmental Security Officer.

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 large and small information systems, *see below*. The distinction is necessary because they require different types of sensitivity statements and threat and risk assessments. For more information on this, consult the Informatics Security Coordinator.)

information system, large a 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 system 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.

microcomputer — a small, personal computer; can be linked with others to form a LAN.

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 device 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.

regional security representative the person who represents the Departmental Security Officer in all security matters concerning the local region.

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 secured 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 a 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.*

D

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 Software				
Monitoring Compliance				
Planning				
Backup and Contingency Procedures				
Copyright				
Integrity Controls				
Contracting for Services and Supplies				

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

FP PU 0021-92-03