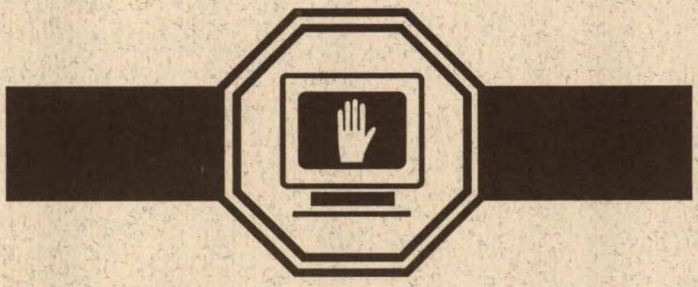
ISTC Staff Handbook on Information Technology Security



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

Canada

ISTC Staff Handbook
on
Information Technology Security

PU 0281-91-03

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.

Special thanks are due to the members of the department-wide steering committee who helped develop these handbooks.

TABLE OF CONTENTS

1. INTRODUCTION

Purpose and scope

This handbook is for all staff who use computers, including managers, supervisors, indeterminate and temporary employees, students and contractors of all levels. It describes Industry, Science and Technology Canada's information technology security standards, and suggests ways for staff to safeguard the department's information and equipment assets. The standards and guidelines set out herein cover most situations staff members are likely to encounter, and apply to all equipment and applications used in ISTC.

Everyone who works for ISTC **must** learn and comply with information technology security standards. As you read this handbook, you might find words you don't understand. If you do, consult the Glossary at the back.

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.

If you find concepts or topics you don't understand, or if you need more information, consult your supervisor,

shared-facility manager, information system custodian or local security administrator. If they cannot help, the problem should be referred to your responsibility centre manager, who may consult the Informatics Security Coordinator, Information Management Branch, or the Departmental Security Officer at Headquarters.

This handbook is part of a series of three. ISTC has also issued the *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians* and the *ISTC Handbook on Information Technology Security for Responsibility Centre Managers.* You may consult them for additional information. The other two handbooks include an index for 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 Ministerial 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 damage, and for taking all reasonable precautions against accidental damage. Computer equipment and the data it contains are vulnerable to damage by careless or uninformed people and saboteurs. Valuable items, such as laptop computers and printers, and consumable supplies, such as diskettes, are attractive to thieves. Sensitive records are also attractive, especially to curious or malicious people.

Here is a partial list of the information technology security responsibilities. All ISTC staff **must:**

- follow work site rules about entering security zones;
- lock portable equipment and sensitive records away when the work site is unattended;
- keep passwords private and change passwords periodically;
- help eliminate slip-ups that would allow unauthorized access to information by reporting them immediately;
- follow antivirus procedures and use only virus-free software;
- control classified and designated printouts and photocopies;
- dispose of classified and designated waste correctly;
- comply with copyright laws;
- back up software and data regularly; and
- report security incidents immediately.

You will receive a full explanation of your information technology security responsibilities at your security briefing (*see* 3. Security training).

Responsibility centre manager

The manager of each responsibility centre establishes safeguards for computer equipment, information systems and all data stored in them, and ensures that all staff follow security procedures. Responsibility centre managers may delegate these duties to other managers, local security administrators 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 it follow security procedures. If a local security administrator has been appointed, that person carries out certain delegated security duties of the shared-facility manager.

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.

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 at Headquarters, advises and assists the Departmental Security Officer. This officer has specific functions 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 in computers administered by the Information Management Branch.

Local security administrator

A local manager may assign certain local information technology security functions to a staff member. If there is no local security administrator at your work site, the local information technology security responsibilities will be carried out by a shared-facility manager or an information system custodian.

3. PERSONNEL SECURITY

Security clearance and enhanced reliability check

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.

You **must** complete the documentation required for security clearance or enhanced reliability check when asked.

Your personal security status will be checked:

- by your information system custodian or shared-facility manager before granting you access;
- by your contract manager before your contract begins;
- by your prospective supervisor before you are hired; and
- by your supervisor before assigning you to new duties involving classified or designated information.

Procedures for security clearance and reliability checking are described in the ISTC *Security Policy and Procedures Manual.*

Segregation of duties

To decrease the risk of damage to records and equipment and of security violations and breaches, 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 workplace is very

small or unless you and your co-workers use only stand-alone microcomputers, you should hold only one of the following responsibilities at a time:

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

Security training

Shared-facility managers and information system custodians are responsible for ensuring that staff are briefed on their information technology security responsibilities and departmental information technology security standards. You **must** attend such briefings:

- when you are hired;
- when you are assigned new duties; and
- when new information technology security procedures are introduced.

To reinforce and refresh information technology security knowledge, you should also attend periodic security briefings when they are available.

Relinquishing a position

When your term or contract finishes, when you receive a promotion or transfer or when you give up an ISTC position for any other reason, you **must** complete a routine that includes:

- transferring and archiving records that need to be preserved;
- 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; and
- providing any information the shared-facility manager needs to cancel your passwords and user ID and to close your user account.

If you are an employee who is leaving the department, you **must** complete the Employee Clearance Record form, following the procedure set out in the ISTC *Security Policy and Procedures Manual.*

4. PHYSICAL SECURITY

You **must** carry a valid building pass when you are in an ISTC work site. You **must** show it when asked.

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 personnel 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 secure valuable equipment and attractive items in locked cabinets or offices. If this is not possible, valuable equipment should be attached permanently to furniture with cables or bolts.

Access to security zones

Access to security zones by visitors, including cleaning and maintenance staff, is strictly controlled. Procedures established by the local manager may require them to sign in and out. You **must** escort or appoint an escort for all visitors you invite into a security zone.

If you see an unescorted, possibly unauthorized person in a security zone, you should find out what that person is doing and, if necessary, either escort that person out of the security zone yourself, or call a qualified co-worker or a security administrator to do it.

Deliberate entry to a security zone by an unauthorized person constitutes a security violation. You **must** report any security violations or breaches that come to your attention or that you suspect to your local security administrator, the local manager or the Departmental Security Officer.

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, that information is required to be classified. For example, diplomatic correspondence discussing a technological transfer agreement with a foreign government contains classified information. Cabinet confidences, including Treasury Board submissions, 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 is not particularly sensitive – birthdates, for instance – but it needs enhanced safekeeping because there are legislated restrictions on its use. Other designated information is very sensitive because its release, modification or interruption would threaten the reputation, commercial competitive position or physical safety of an individual, business or identifiable group.

You **must** safeguard classified or designated information in your custody or when you are working with it according to its degree of sensitivity.

The ISTC *Classification and Designation Guide* will tell you how to assign the correct security levels to records. Consult your supervisor or your local security administrator for help.

Marking classified and designated records

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

If you are creating a record containing classified and designated information, you **must** mark the record 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.

When you put sensitive records on paper or machine-readable media, you **must** use file folders or labels that 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

When you find a record containing sensitive information that has not been marked with the correct classification level or designation:

- if you are the custodian of the record, you **must** classify or designate it yourself, remembering to store it correctly after marking it; and
- if you are not the custodian of the record, you **must** take it to its custodian, your supervisor or the local security administrator to be marked and stored appropriately.

Safeguard requirements for classified and designated records

The safeguard requirements for classified and designated records are set out in Appendix F of Deputy Minister Directive 70-1 in the ISTC *Security Policy and Procedures Manual*. 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).

Access to classified and designated information systems and records stored in computers is given only to authorized users (*see* 8. Controlling Access to Information Technology Systems). You **must not** print classified or designated documents on printers that are located where unauthorized people can see the printout.

Consult your supervisor, local security administrator or local manager if you need help or more 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** declassify or downgrade them. Sensitive records in your custody should be reviewed periodically to keep their security levels current and correct.

Disposal of classified and designated waste

You **must** ensure that classified and designated records that you no longer need are destroyed so that no sensitive information can be recovered by an unauthorized person. Staff in the regions **must** arrange disposal with their local security administrator. Headquarters staff **must** arrange disposal with the Security and Safety Directorate.

You **must** submit paper documents, damaged machine-readable media such as diskettes and tapes, and 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 using a hard disk for other purposes, you **must** remove all sensitive records from it. Software that wipes or overwrites 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 your local security administrator, your shared-facility manager or the Informatics Security Coordinator for recommended products and advice.

6. ADMINISTERING INFORMATION TECHNOLOGY SECURITY

Written procedures

Each information system, data base, shared facility or work site that uses computers **must** have written procedures that cover information technology security.

Refer to your local security procedures for information on these topics:

- responsibilities;
- reporting 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;
- 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.

7. VIRUSES

A virus is a destructive program that can be loaded onto a computer in two ways:

- deliberately, by a mischievous or malicious person who wants to disrupt or destroy the system; or
- inadvertently, by a person who has not followed security procedures.

Viruses replicate and append themselves to other files, programs or diskettes, and they are spread when someone downloads an infected file or program or uses an infected diskette. Viruses are sometimes devised to be triggered by a predictable computer event, such as a date change or other routine operation.

Viruses can damage and destroy data, software and computer hardware. They are particularly destructive when introduced to a LAN or a mainframe.

Basic precautions

There are no practical ways to make a computer immune to viruses, but by following security standards, staff can lower the risk almost to zero. You **must** systematically use a recommended, up-to-date antivirus scanning program:

- regularly for all machine-readable media in your custody, including diskettes and tapes, hard disks in servers, removable hard drives, microcomputers and portable computers;
- before copying and using all incoming diskettes, including diskettes from your home computer and new, shrink-wrapped, licensed software;
- before using all files and programs received through communications lines; and
- before using all new equipment and equipment returned from maintenance.

When you obtain diskettes or programs from outside sources, you **must:**

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

When you access outside systems such as bulletin boards, you **must** consult your shared-facility manager first. Preferably, access public systems only from a standalone microcomputer or download files only onto diskettes that will be scanned before use.

Consult your shared-facility manager on whether you need to scan files that you receive attached to electronic mail messages. Consult your shared-facility manager or the Informatics Security Coordinator about antivirus programs and for advice on the safest ways to use modems.

What to do on detecting a virus

Some viruses announce themselves by displaying a message or an unusual graphic on your monitor. Others have no displays, but cause the computer to do something unusual. The most insidious viruses leave only a trail of corrupt data, blank disk space where data should have been, or damaged hardware to indicate that they have been at work.

If you suspect that your computer has a virus, you **must** stop using the computer immediately and call your shared-facility manager. If you work on a standalone microcomputer, you **must** call the Informatics Security Coordinator or the Departmental Security Officer *immediately*. Speed is essential; the longer you delay in reporting 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, to identify the source. If a virus remains in any file, anywhere in your system, it will appear again.

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 managers use several methods to achieve this, including:

- limiting access to sensitive data stored in multi-user computers to authorized users identified by user identifiers and passwords;
- requiring each user to have a unique user identifier 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

A user identifier (user ID) is a unique code that is assigned to you so the computer can identify you and allow access according to your established privileges.

Passwords

In this handbook — and in general data-processing operations — a "password" is a unique character string that you need to key in before a computer will allow you to

access specific data or software. It is not the WordPerfect™ "password" feature, which is, in fact, a simple form of encryption.

You **must** change your passwords:

- at least monthly, if you use TOP SECRET data; otherwise, at least quarterly; and
- if the shared-facility manager asks you to change it.

As well as following these rules, you can and should change your password whenever you think you should.

You **must** keep your passwords private to prevent unauthorized access.

If you leave the work site permanently, your passwords will be cancelled.

You **must** choose passwords that are:

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

For example, you could use the last three letters of two different words, or the first four letters of a word and two random digits. You **must not** use dates or real words, especially names — they are too easy to figure out.

Never record passwords in readable format. This means you **must not:**

- record them in a computer, except in encrypted form;
- embed them in information system software code;
- include them in unsecured automatic logon procedures stored in any computer (see your shared-facility manager if you need details);

- post them anywhere in sight, especially not on your desk or computer (yes, there really are people who do this);
- write them on a slip of paper you keep in your files, briefcase or wallet; or
- give them to anyone else, except your local security administrator or, if yours is a critical computer function, a backup staff member.

If you have to write passwords down, here are some suggestions:

- write them on a piece of paper, seal the paper into an envelope and store the envelope in a locked cabinet or safe; or
- ask your local security administrator to keep them for you, under appropriately stringent control.

Administration of access controls

When you are assigned a user ID and passwords, especially if you will be working on a LAN, you **must** sign an acknowledgment that you agree to obey the terms and conditions established for your facility.

At least once a year, you will be asked to provide written verification that you still require and are authorized to have computer access.

Access suspension

It is strongly recommended that user IDs and passwords be suspended automatically after three invalid access attempts. This means that after the third time you try to access files or applications for which you do not have privileges, all your computer privileges may be withdrawn while the situation is investigated.

Also, if you do not use your user ID and passwords for a long time, they may be suspended automatically.

Therefore, if you find that your user ID or passwords do not work, contact your information system custodian or shared-facility manager.

Automatic logoff

As a security measure, computers may be programmed to log off terminals automatically when they have been inactive for a predetermined period. If you find that your terminal has been automatically logged off, just log on again and access will be restored.

Storing machine-readable records

Removable machine-readable media

If you have in your custody removable machine-readable media (portable computers, removable hard disks, 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).

Deletion will 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).

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 such hazards as fire and vandalism.

Fixed hard disks

You **must not** store classified and highly sensitive designated information on the hard disk of your computer, even if it is a standalone microcomputer kept in a security zone. Keep it on diskette and store it in an approved security container (see 5. Information Security). Consult your security administrator or the Informatics Security Coordinator for help or more information. 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 offer only minimal security but you should use them if they are available. They can prevent unauthorized people from using your computer, lowering the risk of damage to your files from user errors or viruses. Computer locks and password protections can be overcome, however, and a hard disk can even be removed from the machine. If a computer in your custody has no adequate safeguards, you **must** ensure that sensitive records are wiped from its hard disk or overwritten.

Encryption by a commercially available package approved by the Departmental Security Officer may be an adequate safeguard. If you choose this method, you **must** ensure that one other qualified person has the code key. Consult the Informatics Security Coordinator for advice and recommended products.

Certain software packages, including WordPerfect™, can back up files automatically. This is usually done in 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 you exit the program.

When you use such a product to process sensitive information, and if the program does not encrypt your record as you create it, you **must** ensure that the automatic backup is directed to a diskette. Then you **must** remove and store the diskette in an approved security container. If you are not working with encryption software and you cannot redirect the backup, you **must** disable the automatic backup feature and periodically save the file on a diskette. Then you **must** store the diskette in an approved security container.

Deleting files from your hard disk will not safeguard the sensitive information they contain. Consult your shared-facility manager for information about programs that wipe or overwrite files, destroying them completely (*see* 5. Information Security).

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 a portable computer unattended where it can be stolen. It is particularly important to 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), you **must not** use the original software in regular operations. If possible, store original software (off-the-shelf or custom-written) in a secure place to prevent damage and unauthorized modification.

Communications security and computer security

Communication equipment and lines that transmit sensitive data require the same level of safeguard as the computers that process the same data. Electronic mail is a service that uses communications lines.

Transmitting sensitive information

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** use encryption or some other safeguard approved by the Departmental Security Officer when transmitting classified and highly sensitive designated information, unless a threat and risk assessment indicates otherwise.

Consult your shared-facility manager or the Informatics Security Coordinator about the telecommunications safeguards available at your work site.

TEMPEST

Communications and data processing equipment are called TEMPEST-compliant when they are built so they 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, if you do not work in a shielded room – that is, a room built to prevent electromagnetic emissions – you **must** use TEMPEST-compliant equipment to store, process and transmit 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, 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.

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 information during transmission or in storage. There are several off-the-shelf encryption applications varying in the degree of safeguard they provide. Consult the Informatics Security Coordinator for advice on choosing and using encryption products for designated information. For encryption products for use with classified information, consult the Departmental Security Officer, who approves all encryption products used in ISTC.

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

All staff **must** observe the security requirements of all data they download and upload, and ensure that the receiving computer and the communication method meet those security requirements. Consult the information system custodian and the shared-facility manager for information.

You **must** download and upload designated records only to secure systems.

Dial-up lines

A dial-up line is the easiest route into a computer system for hackers. ISTC computers with dial-up lines are to be safeguarded by additional verification procedures. Consult your shared-facility manager or the Informatics Security Coordinator on using dial-up lines.

9. MAINTAINING HARDWARE AND SOFTWARE

Authorization

Maintenance work may be done only after it has been properly authorized. When somebody comes to work on equipment in your custody, you **must** check for authorization. Maintenance of TEMPEST-compliant equipment may be done only when it has been authorized by the Departmental Security Officer.

On-site maintenance

Maintenance and support staff who work on equipment used to process sensitive information **must** hold appropriate security clearances, which will be checked by the information system custodian, shared-facility manager or the responsibility centre manager.

Before maintenance staff come in to work on equipment used to process sensitive data, you **must** remove all sensitive data or otherwise ensure that it is not accessed, copied or modified. For example, you can escort maintenance staff and supervise them closely while they work.

You **must** escort maintenance staff working on equipment in your custody that is critical to operations or is used to process sensitive data. If you see unescorted maintenance staff working in a security zone or on equipment used to process sensitive information, you **must** call your supervisor or the shared-facility manager.

Off-site maintenance

Before equipment with hard disks in your custody is sent off-site for maintenance, you **must** ensure that all sensitive data has been removed from it. Consult the shared-facility manager, your local security administrator or the Informatics Security Coordinator.

When equipment is returned to your custody after maintenance, you **must** scan it for viruses and check it rigorously to ensure that its security features have not been by-passed, damaged or compromised.

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. Here are some directions and suggestions for keeping your computer clean and safe.

You **must:**

- protect all magnetic media (diskettes, tapes and hard disks) from magnets and electronic equipment that contains magnets or generates magnetic fields, such as speakers and certain telephones.

You **must not:**

- leave diskettes lying around without their protective jackets;
- bend or staple diskettes;
- touch the shiny surface of a diskette;
- write on a diskette with a sharp instrument; or
- use staples or paper clips on a diskette.

You should:

- use write-protect tabs on read-only diskettes to prevent damage to files;
- keep papers and other items clear of the air vents in equipment to prevent overheating;
- keep food and liquids away from computers and machine-readable media;
- cover or pack up computer equipment when it is not being used, when it is being moved and when the environment is very dusty, such as during renovations;

- follow manufacturers' preventive maintenance instructions;
- install surge protectors to safeguard microcomputers from fluctuations in the electricity supply; and
- ensure that a hard disk is safely parked before moving it or the computer housing it.

11. MONITORING COMPLIANCE

All staff are responsible for monitoring compliance with controls on activities under their authority.

Inspections and audits

To ensure that local practices comply with government and departmental policies and standards, local managers, the Informatics Security Coordinator, the Departmental Security Officer and the Operations Audit Branch conduct periodic information technology security inspections and audits. The Departmental Security Officer may also call in the Royal Canadian Mounted Police Security Evaluation and Inspection Team (RCMP SEIT).

Among other aspects of work site operations, inspectors and auditors study the patterns of user activity and computer operation. For example, they review user access records and transaction logs, computer activity logs and backup records. Inspectors are also interested in whether unapproved or illegal software is used, whether sensitive records are marked and stored correctly, and how office space is organized.

Records and retention schedules

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 some or all of these records:

- hardware updates;
- software updates;

- configuration changes; and
- problems and solutions.

Local managers will assign analysis and filing functions.

If you are directed to keep such records, you should establish a retention schedule so that logs are available for periodic security inspections and audits and are disposed of when they are no longer needed. You **must** keep such logs for at least three months, but it is recommended that you keep them for six months to a year.

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

Reporting security incidents

The disappearance of documents and diskettes, and unusual events such as unaccountable changes to software and data, are security incidents. So that it can be recorded and investigated, you **must** report any security incident you know about or suspect to your local security administrator, shared-facility manager or responsibility centre manager. Use the procedures developed for your work site.

A staff member will be appointed to record security incidents and report them to the Departmental Security Officer. 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.

Refer to Deputy Minister 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.

12. BACKUP AND CONTINGENCY PROCEDURES

Daily backup

Backup is a very important security measure. All users **must** learn the backup schedule that their shared-facility manager or information system custodian has established.

You can lose active files through many kinds of accidents, malfunctions and errors, as well as through viruses and other forms of deliberate damage. You back up your files and software by copying them so you can recreate them, at least to the point of your last backup, should they be lost or damaged. Data and software on standalone microcomputers should be backed up periodically to prevent damage to data and loss of time in reinstalling and reconfiguring software.

Some users may need more frequent backup than the system provides. You can arrange changes in the backup schedule with your shared-facility manager or information system custodian, or learn to do the backups yourself. Your shared-facility manager or information system custodian will show you how.

Here are some alternative types of backups:

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

It is extremely important to check that you have completed your backup procedures successfully. Usually a message is displayed on successful completion. Otherwise, you might find out too late that your backup files are unusable because of some processing error.

Storing data and software backups

You **must** store backup media in a safe place away from the active files. This prevents loss of both the latest backup and the active files in the same incident. If you work with information critical to recovery and operations, or with information that would be very difficult to replace should a disaster hit your work site, you **must** store a backup off-site. The Informatics Security Coordinator will help you arrange secure off-site storage for all machine-readable media.

You **must** record the location of your stored backup data and software accurately. You should also record encryption keys and passwords required to access the data, following the precautions for passwords and key material (*see* 8. Controlling Access to Information Technology Systems).

You **must** keep enough generations of backup data to ensure that you can recover uncorrupted data. Think about how long an error or malfunction can remain undetected in your system. You might have to reprocess old data if you have had a problem in your system for some time. If you have destroyed your old backups prematurely, you will have no valid data to work with.

Recovery

You **must** test your data recovery procedures periodically, and always after modifications to related hardware and software. People have lost months of work because, although they backed up their data religiously, they could not recover it after a routine software update had made their backup data incompatible with their system.

Contingency procedures

You **must** learn your functions under contingency plans prepared for your work site. The contingency plan sets out procedures for you to follow to help limit the damage done by a loss of computer resources. Your supervisor will brief you on your responsibilities under the contingency plan. The contingency procedures may provide for reduced service by the affected system, full service by a backup system, or service with no computer resources at all.

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 in only one computer at a time.

Anyone who copies licensed software for an unlicensed user is liable under the *Criminal Code* of Canada.

Staff members' responsibilities

ISTC complies with copyright legislation without exception. You **must** conform to the terms of the licence when copying software. You **must not** use illegal copies of licensed software on ISTC equipment.

When you begin to work for ISTC or when you are granted computer privileges, you may be required to sign an undertaking to copy software and proprietary documentation only as authorized under the licence.

14. RESOURCES

References

The ISTC *Security Policy and Procedures Manual,* which comprises the *Classification and Designation Guide* and the Deputy Minister 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.

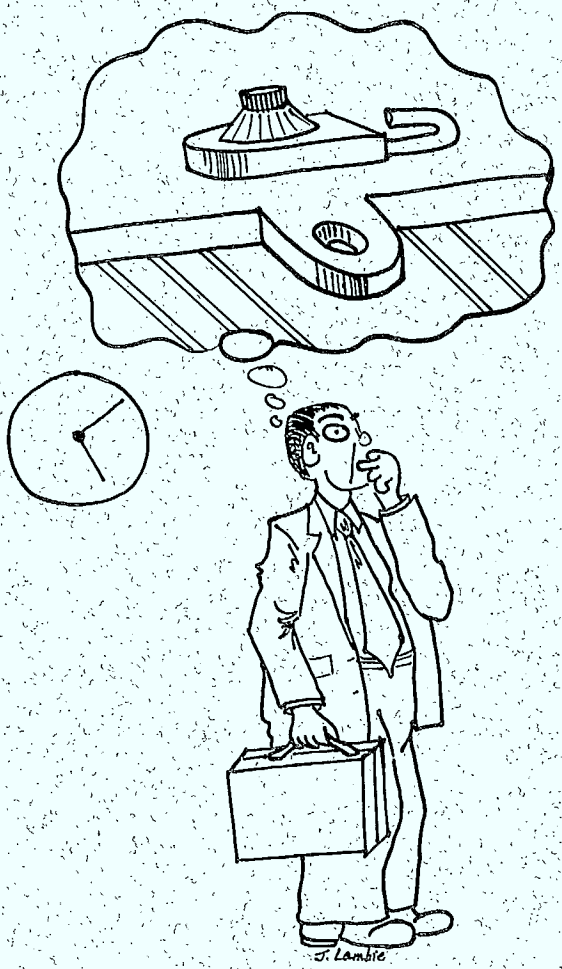
Information and Administrative Management – Security, better known as the Government Security Policy (actually the title of one of its sections), is a Treasury Board manual. It also contains the Interim EDP Security Standards (GES/NGI-14). This is also available from the Departmental Security Officer 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 handbooks in this series, each of which contains a consolidated index to the entire series. The *ISTC Handbook on Information Technology Security for Shared-facility Managers and Information System Custodians* and the *ISTC Handbook on Information Technology Security for Responsibility Centre Managers* are available from the Departmental Security Officer or the departmental library.

Resource personnel

If you have questions about information technology security, consult the:

- shared-facility managers;
- information system custodians;
- Informatics Security Coordinator, Information Management Branch; and
- 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 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.).

hacker common term for a person who compromises or evades safeguards to gain unauthorized access to computers.

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 — 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.

information system custodian — 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 — 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 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.

responsibility centre manager 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 schedule that states how long records, such as computer access logs, must be kept 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 material that is classified or designated or should otherwise not be made available to unauthorized people.

shared-facility manager 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.

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

unauthorized person 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.

INDEX

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				
Care of Computers and Machine-readable Media				
Monitoring Compliance				
Backup and Contingency Procedures				
Copyright				

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