Technical Security Standard

for

Information Technology

(TSSIT)

August 1997

Également disponible en français

FOREWORD

This document, titled "Technical Security Standard for Information Technology" (TSSIT), is designed to assist users in implementing cost-effective security in their information technology (IT) environments. The purpose of TSSIT is to set out the detailed administrative, technical and procedural safeguards required in an IT environment in order to implement the requirements of the "Security" volume, *Treasury Board Manual*, herein referred to as the "Security Policy of the Government of Canada" (GSP).

This document is a technical-level standard for the protection of classified and designated information stored, processed or communicated on electronic data processing equipment. Government information is to be adequately protected through good, basic information management and physical and material management procedures.

This technical standard has been developed, approved and issued pursuant to the lead agency role of the Royal Canadian Mounted Police as stated in the guidelines to the GSP. As such, TSSIT is third-level documentation as outlined in the GSP, Chapter 2-1, "Security Organization and Administration Standard". Terminology used in TSSIT has the same meaning as the definitions in the GSP Glossary (Chapter 1-1, Appendix C).

As permitted by the GSP, when applying standards, departments may decide, on the basis of a threat and risk assessment and after consultation with the lead security agencies, to substitute alternative measures. When substituting alternative measures, care must be taken not to compromise the consistency, and therefore the integrity, of government-wide protection measures.

.

Advice and guidance on applying this standard can be obtained from the departmental security authority and from the lead agencies.

PAGE

1. INTRODUCTION

1.1 Purpose

This document, Technical Security Standard for Information Technology (TSSIT), is intended to assist departments in achieving a minimum level of security for classified and designated information and assets and is based on the principles and requirements of the "Security Policy of the Government of Canada" (GSP).

TSSIT is used by the RCMP Security Evaluation and Inspection Team (SEIT) as evaluation criteria for system reviews (computer systems and computer-based networks including local area networks).

1.2 Scope

The level of security established by TSSIT requirements not only protects a department's assets, but also provides assurance that shared assets will receive a minimum level of protection regardless of the location.

Diverse applications and variation in technical implementations make it impractical to provide specific and detailed safeguards for every possible Information Technology (IT) situation. Additional safeguards are to be applied based on a threat and risk assessment (TRA).

Further, the safeguards detailed in this document do not adequately cover the processing of Top Secret information or aggregates of information necessitating a classification of Top Secret. When it is necessary to process such information, a TRA is to be used as the basis for establishing the security requirements and the relevant departmental security authority must be contacted to determine appropriate additional protective measures in conjunction with the Technical Security Branch (TSB) of the RCMP and other security authorities as required.

TSSIT applies to all government departments listed in Schedule I, Parts I and II, of the Public Service Staff Relations Act, and to the Canadian Forces, the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS). It also should be applied contractually where government information is processed by the private sector. This can be accomplished with appropriate contract security clauses based on TSSIT.

Consistent with changes in policy or technology, TSSIT will be reviewed and amended as and when necessary. A comprehensive review will be conducted at least every five years consistent with requirements identified in the GSP.

Questions concerning the application or interpretation of this standard, and suggestions concerning amendments should be directed to your departmental security authority, who may refer such questions and suggestions to:

Officer-in-Charge
Technical Security Branch
Technical Operations Directorate
Royal Canadian Mounted Police
1426 St. Joseph Boulevard
Gloucester ON KlA 0R2

1.3 Documents

References are listed at the end of this publication.

1.4 General Requirements

IT security is the protection of systems, information (data) and services from accidental and deliberate threats to confidentiality, integrity and availability. IT security is considered to consist of seven components: administrative and organizational security, personnel security, physical security, hardware security, communications security, software security and operations security. These components apply to all types of systems from personal computers to local-area networks, wide-area networks, mini-computers and mainframes. Some of the criteria are technology specific but the intent is applicable to all environments. For the purpose of this document, a network is a system consisting of a connection of computers and devices using communications technology. Specific network issues including architecture, management, interconnection and operating systems are integral parts of the above components.

TSSIT is generic in nature and designed to provide security for information technology applications in general. There are, however, some network applications, such as E-MAIL and the use of INTERNET, which provide special challenges since the information passes through systems and is stored on systems which are often beyond the control of the owner and intended users of the information. Although, in these situations, confidentiality and integrity can be protected using encryption, it is very difficult to provide measures to protect availability. Careful consideration must be given to the level of information processed on these systems and the provision of measures external to the public network and service providers.

The GSP makes departments responsible for the protection of sensitive information and assets, including information technology systems, based on threat and risk assessment and

the application of minimum standards. While complete security is generally considered unattainable, cost-effective safeguards can be chosen which will adequately reduce the risks to an acceptable level.

The requirement for security implies the existence of an internal organization consisting of positions with defined responsibilities which are occupied by personnel who have received IT security training and who will be responsible in attending to security concerns. The requirement for such positions will depend on the size of the organization, e.g. in smaller organizations these responsibilities could be carried out as part of the duties of some other function. The fundamental elements of such organizations are defined in Administrative and Organizational Security (Chapter 2).

Security must be predicated on the loyalty and reliability of all personnel involved. The methods to be used in determining such attributes and in ensuring that personnel are made aware of their security responsibilities are contained in Personnel Security (Chapter 3). The physical and environmental requirements which are necessary to isolate the IT environment from extraneous factors are outlined in Physical and Environmental Security (Chapter 4).

Engineering of systems must follow accepted practices to ensure that security features are integrated and that there is a level of assurance or confidence in their effectiveness. These practices include verification of the implementation of security requirements defined in the threat and risk assessment and the approval to release the system for use. This is sometimes called certification and accreditation. Chapters 5 through 8 (Hardware, Communications, Software, Operations) deal with internal security features provided by systems and the security management of these features.

1.5 System Operational Considerations

1.5.1 General

It will often be desirable to mix applications and data of different sensitivities on a single system or network. Ideally, it would be convenient to identify explicitly the various mixes of sensitivities which could be accommodated without undue risk in any given type of system. Unfortunately, since the combinations of sensitivity and technical implementations are numerous, identification of such mixes is virtually impossible. Each individual configuration and mix must be analyzed for appropriate controls.

The primary criterion in the choice of a system must be the acceptability of the others with whom the system resources are shared. It must be assumed that a knowledgable user will find ways to circumvent normal protective mechanisms if sufficient motivation exists. For this reason, if the other users cannot be identified, or if they are known but are not totally

acceptable, sensitive resources should not be shared without the strict controls of a multi-level environment.

Conversely, if all users of a system are known and identifiable and can be allowed to legitimately gain access to any information on the system, they can be considered singly and collectively to be responsible for the protection of the information. The security concern is therefore minimized and efforts can be concentrated on ensuring that unauthorized persons cannot gain access.

Often, even though users are all known and acceptable, they cannot be permitted access to all system and data resources because they do not share a common need-to-know. Although a security screening process is in effect, it alone cannot be expected to ensure that all users can be explicitly trusted. Furthermore, system isolation mechanisms may fail, causing an inadvertent unauthorized disclosure.

In such cases, it is sometimes possible to provide third party intervention between users and the system. While this may have the effect of increasing the number of personnel required, it provides the capability of manually monitoring system use and improving the separation-of-duties concept. The rules under which the third party intervention is applied can be set to match the system sensitivity.

If third party intervention is not possible, then most of the security mechanisms must be based on the automated responses of the system. For example, if the risk in a particular environment is high, then systems with high assurance levels for protective mechanisms should be used.

Finally, one must examine the capability or privileges granted to users. Compensatory controls can be applied to some privileges. For example, the privilege of being allowed to update transactions on a system can be coupled with controls which provide auditability of transactions. However, in general, if users are allowed to introduce instructions into a system by utilizing compilers, assemblers, interpreters or translators, the possibility of deliberate compromise of a system is greatly increased. For this reason, programming and the introduction of programs (eg. applets in Java) should not be allowed on highly sensitive systems during production periods and must be controlled at all times.

It is these conditions which will be assessed in determining the level of information that may be processed on the system without compromising the confidentiality, availability and integrity requirements. The statement of sensitivity, which contains the confidentiality, integrity and availability requirements for an application and the intended user base, must therefore be taken into consideration when determining an acceptable "Mode of Operation" for processing an application.

1.5.2 Modes of Operation

This section describes the three modes of operation. Although the differences in the three modes are based on confidentiality requirements, processing in any given mode also has an effect on the availability and integrity requirements of computer systems and networks.

Dedicated Mode

A system is operating in the dedicated mode when all the following statements are satisfied concerning the users with access to the system, network, its peripherals, remote equipment, or hosts.

- Each user has been subjected to the appropriate level of personnel screening for all information on the system or network.
- Each user has formal access approval and has signed a non-disclosure agreement for all information stored and/or processed on the system or network.
- All users have an operational need-to-know for all information contained on the system or network.

System-High Mode

A system is operating in the system-high mode when all the following statements are satisfied concerning the users with access to the system, network, its peripherals, remote equipment or hosts.

- Each user has been subjected to the appropriate level of personnel screening for all information on the system or network.
- Each user has formal access approval and has signed a non-disclosure agreement for all information stored or processed on the system or network.
- All users have an operational need-to-know for some of the information contained on the system or network.

Multilevel Mode

A system is operating in the multilevel mode when all the following statements are satisfied concerning the users with access to the system, network, its peripherals, remote equipment or hosts.

- Since different levels of information are processed on the system or network, authorized users have been subjected to different levels of personnel screening, depending on the level of information to which they require access. For example, some users may have been screened to Level II (Secret) while others may have been screened only to Reliability.

- All users have been subjected to the proper personnel screening level and the appropriate formal access approval, e.g. signed non-disclosure agreement, for the information to which they have access.

- All users have an operational need-to-know for the information to which they have access.

The selection of safeguards for each mode depends on a number of interrelated factors identified by a TRA, including sensitivity level, user access requirements and external communications. For example, basic safeguards for a system in the System-High Mode processing sensitive information at the Protected-A level could include assignment of security responsibilities, contingency plans, enhanced reliability screening for users, physical access control of servers and work areas, logical access control functionality and controlled dial communications.

1.6 Security Summary Table

Many security components must be considered when processing government information. It is therefore essential that all aspects of the IT environment be evaluated in relation to the security requirements when selecting safeguards. The Security Summary Table, which is intended as a guide only, highlights topics to be considered when determining the safeguards required in an IT environment. The table is a summary of procedural, personnel, physical and environmental, system and communications safeguards. These areas are complementary, and no one area is more important than another.

The three fonts used in the text of the table reflect increasing security concerns within a security area. The regular font, *italic* font and SMALL CAP font indicate safeguards increasing from basic to more sophisticated protection. There is no ranking or intended order within each font.

Some topics are repeated in different areas in the table, e.g. "Training" and "Access Controls". This repetition indicates the topic is integral to each area in which it is found. More details on the topics listed in the Summary Table are contained in the various chapters of this document.

INFORMATION TECHNOLOGY SECURITY SUMMARY TABLE

	CONFIDENTIALITY	**AVAILABILITY**	**INTEGRITY**
	Regular/ *Italic*/ SM CAP ⇓ Increasing Protection	Regular/ *Italic*/ SM CAP ⇓ Increasing Uptime	Regular/ *Italic*/ SM CAP ⇓ Increasing Accuracy
PROCEDURAL • Administration • Organization	Assignment of responsibilities Separation of duties Classification procedures System Development Life Cycle Standards/policies Business resumption plan Statement of sensitivity Security clauses in contracts	Log review Backups & recovery Written procedures System Development Life Cycle Contracts of • Hardware • Software • Communications Specify • Maximum downtime • Critical minimums Contingency planning Business resumption plan	Change control Media marking Log procedures and review Verification Security audit Testing
PERSONNEL	Training awareness Correct screening/clearances Termination procedures Security clauses in contracts *Separation of duties* *Need to know* MUTUAL ACCEPTABILITY ACCESS VERIFICATION	Training Designated employees Backup personnel specified *Emergency Response Team* RECOVERY TEAM	Training Job description Job responsibilities Termination procedures ACCESS AUTHENTICATION
PHYSICAL & ENVIRONMENTAL	Access controls • Physical • Logical *Doors correctly secured* *Walls slab to slab* *Waste disposal* INTRUSION DETECTION SYSTEMS VERIFICATION OF AUTHORIZATION	Environmental controls Fire protection *Offsite storage* ALTERNATE SITE	Environmental controls *Physical access controls* *Transportation of media*
SYSTEM • Operations • Hardware • Software	System access control File access control Separation of • Development • Testing • Production Trusted computing at C1/C2 level *Separation of physical media* *Transaction logging* *Audit* *Restriction of privileges and capabilities* *Trusted computing at B1/B2 level* ENCRYPTION TRUSTED COMPUTING AT B3/A1 LEVEL TEMPEST	Maintenance Change control Inventory HW/SW Offsite backup of both system SW and data Minimum configuration *Uninterruptible power supply* *Hardware redundancy* ALTERNATE FACILITIES (CONTINGENCY PLANNING)	Change control Restriction of privileges and capabilities Configuration control Maintenance *Range checks* *Value checks* *Error detection* *Error correction* CHECKSUMS LOGGING - ERRORS AUDIT JOURNALS AUTHENTICATION DIGITAL SIGNATURE
COMMUNICATIONS	Configuration Surveillance Log review Change control *Access control* *Authentication* *Approved TYPE II encryption* *Tempest*	Configuration Change control Log review Specify • Minimum downtime • Critical minimums *Alternate routing*	Configuration Change control Surveillance Error detection Re-transmission Log review

INFORMATION TECHNOLOGY SECURITY SUMMARY TABLE			
	CONFIDENTIALITY Regular/ *Italic*/ SM CAP ⇓ Increasing Protection	**AVAILABILITY** Regular/ *Italic*/ SM CAP ⇓ Increasing Uptime	**INTEGRITY** Regular/ *Italic*/ SM CAP ⇓ Increasing Accuracy
	HIGHGRADE (TYPE I) ENCRYPTION	DUPLICATE SERVICES	AUTHENTICATION

2. ADMINISTRATIVE AND ORGANIZATIONAL SECURITY

2.1 Information Technology Security Organization

2.1.1 Appointment of Security Personnel

1. If you are a government department, appoint:

   - a departmental security officer (DSO),
   - an IT security coordinator, and
   - if you have COMSEC concerns, a COMSEC authority.

2. If you are a private sector organization doing contract work for the federal government, appoint:

   - a company security officer (CSO),
   - when deemed necessary, an IT security coordinator, and
   - if you have COMSEC concerns, a COMSEC officer.

3. Appoint an IT security representative for each physical location.

4. Other security designates can be appointed with responsibilities that include the security aspects of personnel, physical and environment, hardware, software, operations and communications.

2.1.2 Responsibilities of Security Personnel

1. The DSO should have a functional reporting relationship to the Deputy Minister or head of the organization for reporting security issues where warranted.

2. The DSO is responsible for the development, implementation, maintenance, co-ordination, and audit of departmental IT security policies, standards and procedures, to ensure the:

   - appropriate security clearances/screening of personnel handling classified/ designated or other sensitive information;
   - adequacy of physical security; and
   - adequacy of IT security.

3. The IT security coordinator should have a functional reporting relationship to the DSO and be responsible for:

- planning and conducting regular IT TRAs;
- preparing evaluation reports;
- developing IT security procedures, proposals for safeguards and contingency plans;
- as a minimum, annually reviewing IT security measures and contingency plans;
- addressing IT security incidents and ensuring the timely application of corrective measures to prevent possible recurrence;
- participating in the development and testing of IT contingency plans;
- participating in business resumption planning;
- alerting the DSO to potential and actual security problems;
- designing and implementing an IT security awareness program;
- reviewing contracts for inclusion and adequacy of IT security clauses;
- addressing IT security deficiencies found during investigations, reviews, etc.; and
- determining the action to be taken whenever a safeguard is bypassed.

4. The COMSEC authority should be responsible for:

- custody of cryptographic material and custodial records;
- assisting in IT TRAs and ensuring the implementation of any resultant recommendations and/or corrective measures;
- developing COMSEC procedures;
- checking COMSEC practices and correcting deficiencies;
- alerting the DSO to potential and actual COMSEC problems and ensuring that corrective measures are taken;
- instructing personnel handling COMSEC equipment to observe security measures;
- reviewing contracts for inclusion and adequacy of COMSEC security clauses;
- addressing COMSEC security incidents and ensuring the timely application of corrective measures to prevent possible recurrence;
- ensuring the disposal and destruction of superseded COMSEC material as stipulated in current doctrine and procedures; and
- advising on the action to be taken whenever a COMSEC safeguard is bypassed.

2.2 Information Technology Security Administration

2.2.1 Security Policy and Procedures

1. Develop and issue written IT security policy and procedures.
2. Departments should maintain a reference library consisting of the GSP and TSSIT and documents referenced therein. In addition, the following documents should be maintained:

- statutes affecting the security of information within the department;
- "Fire Protection Standard for Electronic Data Processing Equipment," Treasury Board Manual, Occupational Safety and Health, Chapter 3-3;
- local fire regulations;
- for private sector only, Industrial Security Manual, Supply and Services Canada, and the COMSEC supplement (where required); and
- any other documents deemed relevant to the security of the department.

2.2.2 Classification and Designation of Sensitive Information and Assets

1. Develop a classification and designation guide that contains procedures for the classification, declassification, designation and downgrading of IT information and assets.

2. The classification and designation guide should specifically address all types of information processed in the IT environment and be reviewed annually.

3. Classify and designate IT assets according to their confidentiality, integrity, availability and value.

2.2.3 Statements of Sensitivity

1. Prior to an application being processed on any computer system, prepare a statement of sensitivity specifying the security classification or designation, availability requirements, and integrity concerns.

2. Statements of sensitivity should be available to persons responsible for the security of the IT system.

2.2.4 Contracting

1. Specify security requirements in all contracts with external organizations where those contracts affect sensitive IT services, information or equipment.
2. Use the Security Requirements Checklist (SRCL) to define the security

requirements for contracts for which Public Works and Government Services Canada (PWGSC) is the contracting authority. This also applies to call-ups against standing offers where the standing offers or call-ups contain security requirements.

3. When your department is responsible for the security aspects of a contract, check the security status of the contractor with PWGSC and inform PWGSC when you have determined that the contractor meets the appropriate security requirements. Document the decision that a contractor meets appropriate security requirements.

4. When your department is the contracting authority, request the Security Evaluation and Inspection Team (SEIT) of the RCMP to determine whether the contractor's IT facilities processing designated or classified information comply with the contract security clauses.

5. Private sector facilities supporting the processing of sensitive government information, or supporting an essential government service should be required by contract to ensure that:

- employees are completely aware of their security obligations, and
- to the degree possible, services will continue during periods of labour unrest.

6. Where information to be processed at facilities controlled by a contractor could be subject to conflict of interest, contracts should clearly specify the nature of the information to be processed and should require the contractor, its management, key officials and IT employees to declare that there is no actual or potential conflict of interest.

2.2.5 Threat and Risk Assessments

1. Prepare and maintain TRAs that address all IT systems, outline existing and proposed safeguards and describe threats and risks of which account has been taken.

2.2.6 Access Control and Authorization

1. Authorize and control access privileges to system and information resources for:

- users,
- operations personnel,
- maintenance and support personnel, and
- systems analysis and programming personnel.

2. Ensure that, prior to being granted access to system and information resources, each individual signs a witnessed and dated acknowledgement that a specific dated version

of the rules and regulations governing such access has been read and agreed upon. Maintain this acknowledgement for a minimum of one year after the employee terminates employment.

3. Rules and regulations associated with access to system and IT resources should stipulate:

- that system and information resources be used only in direct support of authorized departmental projects, together with explicit exceptions if required;
- the authority required to produce or modify IT executable instructions (e.g., software, command procedures, configuration control);
- the responsibilities respecting the use of user-IDs, passwords, and access control items such as encryption keying material, keys, tokens, locks, and access cards;
- the authority required to modify, delete or add to sensitive data or programs;
- the authority required to access any information or software entity;
- restrictions in the movement, maintenance and use of TEMPEST equipment;
- the authority required to add, move or change communications equipment or software (Note: This authority will be the COMSEC authority for classified or otherwise sensitive communications);
- responsibilities respecting the reporting of security incidents;
- restrictions which limit an individual's access to specific locations, times, systems, files and programs (transactions);
- responsibilities respecting copyright-protected programs and data;
- the authority required to remove hardware, communications, or software products from the premises (both permanently and temporarily);
- responsibilities respecting the backup of critical programs and data;
- that all software and hardware be examined for malicious code, e.g. viruses, prior to initial use;
- that all use of departmental computer systems can and will be monitored for compliance with the rules and regulations; and
- that any violation of the spirit or intent of the rules and regulations can lead to loss of privilege or employment, and to disciplinary action or legal procedure.

4. Implement mechanisms and procedures to audit compliance with the rules and regulations governing access to system and information resources.

2.2.7 Security Logs and Records

1. Maintain a current list of those personnel authorized to access systems and information resources.

2. Identify and document:

- the types of security activities and events to be monitored,
- the method of determining how activities and events are to be monitored,
- the type of records to be kept, and
- how and when the security information is to be reported.

3. Record all suspected security incidents affecting the IT environment and report them to the appropriate authority.

2.2.8 Security Investigations

1. Define the type of event or activity which constitutes a security incident.

2. Document and issue procedures to be followed by an employee who observes or becomes aware of a security incident.

3. Investigate security breaches or incidents and maintain a record on each case. Report, to the Deputy Head, security incidents that constitute a possible breach.

2.2.9 Security Reviews

1. Request reviews of your IT security programs and systems by the Security Evaluation and Inspection Team (SEIT) of the RCMP to determine the security status of your IT facilities.

- Request SEIT reviews according to the following schedule:

  ITS programs and systems involving:

  - classified and extremely sensitive designated information, every 3 years

  - all other designated or otherwise valuable information, every 5 years

- Request a review immediately following a major security incident.
- Request a review immediately, for cause, based on the following security-relevant major events in the system life cycle:

- physical move,
- reconfiguration,
- change in communication controls,
- change in sensitivity of information processed, or
- change in operation.

SEIT will conduct a preliminary review, including a review of any previous SEIT report, the results of which will determine whether a full review is to be carried out, consultation given or such other action taken as is applicable, e.g. further follow-up on a previous SEIT report.

2. Within six months of receipt of the SEIT review report, inform SEIT of your plan to deal with identified problems. Provide SEIT with an annual progress report until all recommendations are successfully completed.

3. Conduct and document an annual security review of IT-related activities.

2.3 Integrity and Availability Measures

2.3.1 Separation of Duties

1. Ensure, to the extent possible, that responsibilities are separated in such a way that no individual has complete control over related critical IT operations. For example, the following duties should be separated: programming, system administration, testing and production.

2. Ensure, to the extent possible, that no individual performs all aspects of a critical process. For example, the functions of data input and processing should be separated.

3. Train employees with privileged access and monitor their activities to ensure appropriate security is maintained during their periods of access.

2.3.2 Contingency Planning

1. Define and document, based on statements of sensitivity, the essential levels of service and the maximum acceptable periods of downtime for IT systems.

2. Assign a processing priority to application systems for the purpose of determining service continuity and backup requirements.

3. Develop, document and maintain plans to ensure the essential level of service will be provided following any loss of processing capability or destruction of the facility.

Ensure plans cover on-site and off-site recovery and, as a minimum, consider:

- recovery from any failure to the system and information resources;
- re-establishment of the IT services, following destruction of the facility providing those services, using none of the systems and information resources contained within the primary facility;
- forced evacuation of the facility;
- strikes in the public and private sectors;
- bankruptcy of critical suppliers;
- loss of critical support systems; and
- identification of essential systems, information resources and personnel.

4. Where contingency plans require the use of facilities not under the control of the department, establish formal agreements or contracts for the use of such facilities and review them annually.

5. Ensure that the implementation of contingency plans does not compromise confidentiality or integrity requirements.

6. Maintain current copies of all contingency plans, procedures and agreements in at least two geographically-separate locations.

7. Test contingency plans annually to the extent practicable and ensure they remain consistent with security.

2.3.3 Critical Human Resources

1. There should be sufficient alternate trained personnel to assure the confidentiality, integrity and availability of critical systems.

TSSIT *Chapter 2 - Administrative and Organizational Security*

2. Identify employees required to support an essential level of service on an up-to-date list and incorporate the list into the contingency plans.

3. Ensure employees identified to take an active role in contingency situations receive training and practice in their assigned duties.

4. Maintain a list of employees whose duties are necessary in the interest of safety and security of the public.

3. PERSONNEL SECURITY

3.1 Security Screening

1. Verify that the appropriate security screening type and level has been specified for each position or contract, according to the highest level of sensitivity of IT systems, information or assets which might be accessed by the person occupying that position or performing the contracted duties.

2. Ensure that personnel and contractors have been security screened to the level specified for their position or contract prior to authorizing their access to sensitive IT systems, information or assets.

3. Maintain a current list of positions requiring access to sensitive IT systems, information or assets, the screening level specified for each position, and the actual screening level granted to the incumbent of each position.

4. If new duties or tasks require an individual's personnel screening level to be:

   - higher:

     - make administrative arrangements to ensure that access to higher level information occurs only after the appropriate screening process is successfully completed;
     - remove the person from those functions if the higher level is denied; and
     - reflect these changes in a Security Screening Certificate and Briefing Form (TBS 330-47).

   - lower:

     - inform the individual of the new access requirements of the position or contract;
     - reflect these changes in a Security Screening Certificate and Briefing Form (TBS 330-47), or Administrative Cancellation Form (TBS 330-25).

   - reactivated after a previous lowering:

     - reactivate the original status or clearance according to Section 4 of Chapter 2-4 of the GSP, Personnel Security Standard; and
     - reflect the reactivated screening level in a Security Screening

Certificate and Briefing Form (TBS 330-47).

3.2 Security Awareness

1. Document and implement a security awareness program. To properly address IT security concerns during development and implementation of the program, ensure there is coordination between security personnel (DSO, ITS coordinator, CSO), managers and human resources personnel.

2. Ensure the security awareness program informs personnel of items which might affect their duties and working environment, such as:

- security features and vulnerabilities specific to IT systems and programs used in the performance of their duties;
- new security issues;
- what constitutes a security breach, violation or concern, and;
- procedures for reporting security breaches, violations or concerns;

through such means as;

- properly-documented IT security briefings;
- security notices, pamphlets, posters, and signs;
- security videos; and
- security training.

3. Conduct security briefings with personnel and contractors who will have access to sensitive IT systems, information or assets. These briefings should include:

- the access requirements of their position or contract;
- their authorized security screening level;
- their responsibilities for safeguarding sensitive information and assets;
- relevant sections of other legislation applicable to their duties; and
- departmental or company IT security rules and regulations.

4. Conduct security briefings in person, where possible, and include a written document outlining the contents of the briefing and date given. The document should be signed by the person briefed indicating receipt of, and agreement to, its contents.

3.3 Training of Personnel

1. Train all personnel on IT security principles, and the features and vulnerabilities of sensitive IT systems, information or assets they have access to during the performance of their duties. This training should be designed specifically for the various employee functions, such as ITS coordinators, system administrators, and system users.

3.4 Transfer of Personnel

1. Document and implement procedures to ensure that when personnel or contractors are transferred by appointment, assignment, deployment or secondment, all their access privileges to IT systems, information or assets are reviewed, then modified or revoked accordingly.

3.5 Termination of Employment

1. Document and implement procedures designed to ensure that prior to termination of an individual's employment or contract:

- the individual is debriefed on continuing security responsibilities;
- access privileges (system passwords, user IDs, combinations etc.) to systems, restricted zones, and IT facilities are revoked; and
- all sensitive security-related items (badges, keys, documents etc.) issued to the individual are retrieved.

4. PHYSICAL AND ENVIRONMENTAL SECURITY

4.1 Facility and Equipment Location

4.1.1 Information Technology Facilities

1. An IT facility is the setting used for the location of IT assets such as mini-computers and mainframe computers, LAN servers and telecommunications centres.

2. Minimize risks to IT systems by choosing facility locations with due regard for such threats as: floods and earthquakes, electromagnetic interference and emanations, criminal activity and industrial accidents. Also consider the ease and effectiveness of controlling access in multi-tenant or public buildings.

For detailed information on site selection refer to *Guide to the Preparation of Physical Security Briefs*, SSB/SG-25.

3. Where site selection cannot compensate for identified risks, implement corrective perimeter security measures. Such measures can include the installation, relocation, or removal of fences, walls, trees, embankments, or other barriers and obstructions, depending on whether they compromise, or enhance, security.

4. Ensure areas containing sensitive IT systems, information or assets are situated so as to minimize exposure to threats such as:

- fire, flooding, water damage, corrosive agents and smoke from adjacent areas;
- explosion or shock; and
- undesirable, externally-generated electromagnetic radiation.

4.1.2. Information Technology Equipment

1. IT systems and media contain concentrated amounts of sensitive government information warranting special attention. Consequently, areas housing these IT systems and media may require additional physical security safeguards.

2. Position information technology equipment handling sensitive information in a manner that prevents unauthorized overview or access. This can be achieved by such means as:

- facing monitor screens away from windows or adjacent areas; and
- appropriate placement of printers, fax machines, and other peripheral

equipment.

3. Where the use of shielded enclosures is necessary, comply with the requirements of *Specifications for the Design, Fabrication, Supply, Installation and Acceptance testing of Radio Frequency Shielded Enclosures* (CID/09/12).

- Install shielded enclosures in a restricted zone (Security Zone as a minimum).

- Locate a shielded enclosure within a restricted zone in such a manner that:

  - the enclosure walls are a minimum distance of 60 cm from the "parent" walls (walls of room housing enclosure);
    Note: If maintaining this minimum distance is impractical, take steps to prevent probing or penetration of the enclosure through parent walls, such as reinforcing these walls.
  - penetrations of the enclosure by external sources, such as pipes and ducts, are kept to a minimum;
  - the doors to the enclosure are situated as close as possible to the centre of the restricted zone in which it is housed; and
  - the enclosure is as close as possible to the grounding point.

4. Where the use of TEMPEST-compliant equipment is necessary, comply with the requirements of *COMSEC Installation Planning (TEMPEST Guidance)* (CID/09/7A).

5. If possible, install and operate TEMPEST-compliant equipment within a dedicated restricted zone, established as a Security Zone as a minimum, and separated from adjacent areas by physical barriers.

6. If the TRA does not support a dedicated restricted zone for TEMPEST-compliant equipment:

- install the equipment in a cabinet designed for such a purpose; and
- lock the cabinet when the equipment is not being used.

7. To prevent compromise of the TEMPEST-compliant equipment or information by unauthorized overview or physical access, position the equipment:

- with monitors facing away from windows or adjacent areas; and
- with printers, fax machines, STU IIIs and other peripheral equipment located in the appropriate restricted zone.

8. Do not move or tamper with TEMPEST-compliant equipment after installation and testing without the approval of the appropriate COMSEC authority.

4.2 Access

4.2.1 Restricted Zones

1. Establish the appropriate restricted zones for areas where sensitive IT systems, assets, information and support utilities will be located. These areas include:

- computer rooms (mini or mainframe);
- LAN-server rooms;
- telecommunications centres;
- shielded enclosures and rooms housing them;
- rooms housing TEMPEST-compliant equipment;
- media libraries;
- mail rooms;
- heating, ventilating and air conditioning (HVAC) system rooms;
- electrical system rooms;
- uninterruptible power supply (UPS) system **rooms**;
- fire protection system rooms; and
- offices and their related computer equipment (PCs, printers, fax machines).

2. Control, authorize and monitor access to restricted zones in a manner appropriate for the sensitivity of material contained, or activities conducted, in those zones.

3. Properly escort and supervise maintenance and service personnel, such as customer-engineers, electricians, and plumbers at all times while they are on site servicing sensitive IT systems. Proper escort and supervision means by someone responsible to the department with enough background, training or qualifications to understand the risks associated with the work being done and to provide assurance that only authorized access to sensitive information or assets takes place.

4. Do not post signs, or display other information, in areas accessible to the general public such as lobbies, waiting rooms and reception zones if the signs or information reveal the purpose or location of restricted zones containing sensitive IT systems, information or assets.

5. If signs are used to identify restricted zones, ensure that they:

- denote the type of restricted zone established (Operations Zone, Security Zone, High-Security Zone);

- are prominently posted at all entrances to the restricted zones; and
- meet the requirements of the *Federal Identity Program Manual.*

4.2.2. Controlling Access

1. Control access to restricted zones by using appropriate methods such as:

   - installing electronic access controls, mechanical combination locksets, or deadbolts;
   - limiting the number of entry points to the minimum required by fire regulations; and
   - situating personnel (receptionists, office employees, guards) at entry points.

4.2.3. Authorizing Access

1. Maintain a list of persons authorized to access rooms specially designed for sensitive IT assets and operations, such as computer rooms, LAN server rooms, telecommunications centres, shielded enclosures and TEMPEST-compliant equipment rooms.

2. Maintain access records for persons accessing IT facilities processing Secret or Top Secret information on the following basis:

   - for personnel authorized to work there, at the start and termination of a scheduled work shift;
   - for all other individuals, upon every access and departure.

3. To ensure that access records maintained for restricted zones are meaningful for security audit purposes, include the following details as a minimum:

   - the name of the person entering;
   - the person's employer or affiliation;
   - the name of the official authorizing entry;
   - the restricted zone entered;
   - date and time of entry;
   - date and time of departure; and
   - if required to verify identity, the specifics of any documentation produced such as a drivers licence or departmental identification card.

4. Ensure that access records maintained for restricted zones:

   - are reviewed by security personnel regularly (daily preferred); and

- are retained for at least one year from the end of the current calender year.

4.2.4 Monitoring Access

1. Monitor access to Security and High-Security Zones continuously, and monitor access to Operations Zones at least periodically, based on a TRA. Monitoring methods include:

- operational personnel working in the area;
- security guards;
- electronic intrusion detection (EID) systems;
- closed circuit television (CCTV) systems; and
- electronic access control (EAC) systems with recording capability.

2. All persons authorized to enter restricted zones should be issued, and required to wear, an approved access badge (building pass or recognition badge).

3. Approved access badges meet the following minimum requirements:

- visually and uniquely associated with the applicable restricted zone or facility;
- visually indicate the status (employee, visitor, trades person) and access privileges of the bearer (e.g. Visitor - Escort Required);
- display a badge control serial number;
- sealed in a tamper-proof enclosure (laminated);
- identify the issuing department by indirect codes, e.g. letters and designs recognizable by authorized personnel, not by name or address; and
- for employees, bear a facial-view coloured photograph or digitized image of the employee.

4. To assist with personal identification while monitoring access, issue approved identification cards to employees and contractors requiring regular access to IT facilities. Approved identification card specifications include:

- name and signature of cardholder;
- facial-view colour photograph or digitized image of cardholder;
- name of issuing department;
- issuing officer's signature;
- expiry date (maximum five years from issue date); and
- pre-printed serial number unique to the card.

5. When implementing an identification card or access badge system within your

facilities, establish procedures for:

- issuing and retrieving cards and badges;
- reporting improper use, damage, loss or theft of cards or badges;
- retrieving cards or badges upon termination of employment or contract, expiration or damage;
- maintaining an inventory of issued cards and badges;
- withdrawing cards or badges for cause (e.g. a higher screening level required, employee suspended or being investigated);
- providing physical protection for blank cards, badges, and the equipment used to produce them;
- destroying all expired or damaged cards and badges; and
- preventing the removal of access badges from the facility or any restricted zones when supported by a TRA.

6. Include the following information in records pertaining to the issue and retrieval of identification cards and access badges:

- date of issue;
- identity of the bearer;
- control number of card or badge;
- expiration date of card or badge; and
- the security screening level of the bearer, if a TRA indicates it is applicable for the facility.

7. Maintain records documenting the issue and retrieval of security-related items such as:

- keys;
- combinations for mechanical/electronic locks;
- cards for card-access systems; and
- padlock combinations.

For further information refer to *Identification Cards / Access Badges*, SSB/SG-27.

4.3 Storage of IT Media and Assets

1. Store sensitive IT media or assets in approved security containers located in the appropriate restricted zone. Containers may not be necessary when a restricted zone has been designed and constructed as an approved Secure Room (Type A, B, C, or D) for such storage.

2. If environmental or fire protection concerns exist for either on-site or off-site

backup storage of sensitive IT media, store the media in containers appropriately designed for such protection.

3. Issue keys and combinations for containers storing sensitive information or assets only to authorized personnel. Ensure that records of issue are maintained.

For further information on storage of sensitive media and assets refer to:

- *Security Equipment Guide*, SSB/SG-20.
- *Construction Specifications, Secure Room C*, SSB/SG-23.
- *Construction Specifications, Secure Room D*, SSB/SG-22.
- Chapter 2-2, GSP, "Physical Security Standard".

4.4. IT Utilities and Services

4.4.1. General

1. Document and implement maintenance procedures, consistent with the manufacturers' specifications, for environmental support equipment such as electrical systems, HVAC systems, UPS systems, and fire protection systems.

2. Maintain records of all environmental support equipment maintenance activities. Retain these records for a minimum of one year; and review them at least annually to ensure that the maintenance performed is consistent with that recommended by the manufacturer.

3. Document and implement procedures to ensure that all environmental support equipment faults are:

- brought to the attention of staff responsible for the operation and maintenance of the IT system; and
- recorded by staff, including the action taken and the final resolution of the faults.

4. Centrally control, authorize and document all changes to environmental support equipment.

5. Utility service lines (hydro, water, gas, oil) providing support to IT facilities should enter the building underground or be physically protected by other means, such as:

- enclosing exposed hydro lines in conduit,
- installing barriers around water and gas mains or meters, and
- locking the covers on fuel tank inlet pipes.

6. Protect utilities and services supporting IT equipment, such as power distribution panels, communications and telephone closets, HVAC systems, and external air intakes that are located outside a facility's restricted zones by:

- securing them appropriately using safeguards such as locks; and
- limiting access to persons with a functional requirement.

4.4.2 Electrical Systems

1. The "Fire Protection Standard for Electronic Data Processing Equipment", *Treasury Board Manual* - Occupational Safety and Health, Chapter 3-3 applies to electrical systems for government IT facilities. Primary areas impacting on security and services include:

- power supply cables,
- exposed wiring and cables in plenum and underfloor spaces,
- service transformers,
- power disconnection for IT equipment in a computer room,
- uninterruptible power supply system (UPS),
- enclosures for unsealed-type battery banks for UPS,
- electrical conductors between IT equipment and UPS if located in different fire compartments, and
- emergency lighting for computer rooms.

2. Ensure that power services for IT equipment comply with manufacturers specifications and, where necessary, are equipped with power conditioners capable of providing a stable power supply.

4.4.3 Heating, Ventilating and Air Conditioning (HVAC) Systems

1. The "Fire Protection Standard for Electronic Data Processing Equipment", *Treasury Board Manual*, Occupational Safety and Health Chapter 3-3. applies to HVAC systems servicing government computer systems.

2. Ensure that HVAC units for computer systems considered either "essential" or "non-essential but of high value (exceeding $1 million)", as defined in the "Fire Protection Standard for Electronic Data Processing Equipment", *Treasury Board Manual*, Occupational Safety and Health Chapter 3-3, provide:

- continuous monitoring and recording of temperature and humidity; and
- appropriate signalling of deviation from acceptable levels of temperature and humidity.

3. Install security screens or filters, as appropriate, to protect external openings for HVAC systems against the insertion of hazardous objects or the intrusion of pollutants.

4. Where criticality of service is a concern, redundant air conditioning capacity should be provided.

4.5 Fire Protection

4.5.1. IT Equipment

1. The requirements of the "Fire Protection Standard for Electronic Data Processing Equipment", *Treasury Board Manual* - Occupational Safety and Health, Chapter 3-3, apply to computer systems considered either "essential" or "non-essential but of high value (exceeding $1 million)".

4.5.2 Record Storage

1. Protect and manage records stored and handled in IT facilities according to the requirements set out in *Record Storage*, FC 311(M). For computer rooms, these requirements include:

- limiting the number of records kept in the room to the minimum daily requirement and storing them in closed metal containers or cabinets;
- storing records essential to operations in containers having a fire-resistance rating of at least one hour;
- storing master records, from which operating or current records can readily be reproduced, in a different fire compartment, or off site in containers

having a fire-resistance rating of at least one hour; and

- after each periodic updating of IT media requiring retention, storing the previous record or generation of data in an approved record-storage facility.

4.6. Destruction of IT Media

1. Destroy IT media containing sensitive information in an approved manner, using equipment listed in the *Security Equipment Guide*, SSB/SG-20. Currently, approved methods of destruction include shredding, disintegration, and incineration.

2. While IT media containing sensitive information is awaiting destruction or in transit to destruction, protect it by:

- safeguarding the media in a manner approved for the highest sensitivity of the information stored on that media, and
- keeping the sensitive media separate from non-sensitive media.

3. Monitor the destruction of IT media containing sensitive information by having the process observed by an employee with a security screening level at least equal to the highest sensitivity of the information stored on that media.

For further information on media destruction and sanitization, see these documents:

- *Chapter 2-2*, Physical Security Standard, Destruction section, *Treasury Board Manual*, "Security" volume, Chapter 2-2;
- *Security Equipment Guide*, SSB/SG-20; and
- *TSSIT*, Operations Security, Media section.

4.7 Offsite Facilities

1. Document and implement departmental plans to ensure that physical and environmental safeguards available at off-site facilities provide at least the same level of security as at the primary site. Such off-site facilities include those used for storage of sensitive IT media, or as backup facilities for critical services.

2. Ensure that off-site storage or backup facilities are not subject to the same physical and environmental threats as the primary site.

4.8 Transport and Transmittal

1. The *Standard for the Transport and Transmittal of Sensitive Information and Assets*, SSB/SG-30, applies to all government departments with such material.

2. Package, transport and transmit IT media such as tapes, diskettes, cartridges and hard drives in a manner that protects against rough handling, tampering, compromise and environmental threats such as extreme heat, cold and humidity. All of these conditions can damage or destroy the media and the sensitive information resident on it. Protective measures include:

- securely packing bulk quantities of IT media in solid containers (usually plastic) designed for that purpose;
- packaging diskettes and cartridges in hard-covered sleeves or cartons before wrapping;
- adequately securing containers with ties (plastic or metal) which can not be opened unless broken, or with padlocks; and
- using vehicles with adequate temperature and humidity controls.

4.9 Evacuation Procedures

1. Document evacuation procedures for IT facilities to ensure personnel safety and to maintain security of sensitive information and assets during and following evacuation. Evacuation procedures should cover as a minimum:

- circumstances under which evacuation is to be implemented;
- a list of facilities or restricted zones subject to these procedures; and
- names and specific security duties of personnel delegated responsibilities during evacuation.

2. Distribute and regularly test evacuation procedures for IT facilities to ensure that:

- assigned personnel are familiar with their duties;
- existing procedures are adequate; and
- security is maintained during and following evacuation.

5. HARDWARE SECURITY

5.1 Administration

5.1.1 Configuration/Inventory

1. Maintain a chart of the current hardware configuration, identifying all hardware units and interconnections (e.g., CPU, peripheral devices, channels, controllers, etc.) and review it at least annually or, as warranted, when changes are made.

2. Maintain a current hardware inventory that identifies: manufacturer/supplier, model number, serial number, revision levels, micro-code levels, and ownership.

3. Where availability is a concern, identify and document the current minimum hardware configuration to support critical applications.

4. Assign and document responsibility for the maintenance of hardware records.

5. Keep a current copy of the hardware records (both operational and critical minimum configurations) at an off-site location.

5.1.2 Contracting

1. Ensure contracts specify the security requirements which apply to the hardware and related services controlled by a contractor or subcontractor, such as:

- access to departmental information:
  - need-to-know principle;
- release of information by the contractor:
  - configuration details;
  - information processed by the hardware;
- protection of data:
  - disposal techniques for media;
  - procedures for maintenance, problem resolution, configuration control and change control; and
- service levels required:
  - define maintenance windows;
  - identify critical hardware;
  - define contingency plans.

2. Ensure the contractor lists all subcontractors to be used on the project.

3. Include in contracts a configuration chart agreed upon by the department and the contractor.

4. Ensure any configuration changes made during the period of the contract are documented, reported, reviewed, and approved prior to implementation and do not reduce the level of security provided. Any exceptions must be approved by the contract authority.

5.2 Security Features

5.2.1 Prevention Features

1. Where locks for hardware are available, maintain them in a secure operating position during normal operation.

2. Control remote diagnostic access at all times.

3. Ensure all essential IT equipment left powered up and unattended has an automatic power-down capability, that will respond to environmental conditions outside the specifications detailed by the supplier, e.g. over-temperature, over- and under-voltage and humidity.

4. Where control keys/buttons are exposed, they should be protected from inadvertent operation, e.g., disk drive start/load buttons, write lock buttons, start buttons.

5. Ensure systems processing particularly sensitive designated information or above, using authorized remote input/output (I/O) units, are capable of uniquely identifying each user or unit by hardware means or other alternatives such as:

- smart cards;
- dedicated communications, if the I/O units are contained within secure zones;
- approved encryption methods; or
- manual intervention.

Note: Ensure any changes to the hardware mechanism are possible only by replacing that mechanism.

6. A TRA should be used to determine if TEMPEST-compliant equipment or alternate methods approved by the COMSEC authority are necessary to process classified or designated information.

7. The combination of hardware and software features or techniques should provide an environment capable of isolating and protecting users. As a minimum, the features or techniques should provide for:

- a set of privileges restricted to the system software which are not available to the user;
- control of computer system privileges, protective features, and controls such that only the system software may effect changes;
- use of only the system software to execute a halt or physical I/O instruction; and
- positive action when confronted with an undefined instruction bit pattern, illegal memory request (out of bounds to the current process), or hardware errors. Such action may include generating an interrupt.

8. Check the system's protective mechanisms periodically to ensure they are functioning properly. This could include checking the capability of the system to prevent unauthorized:

- access to the system,
- access to data resources,
- access to residual data,
- use of privileged capabilities, and
- read/write capability outside allocated memory bounds.

5.2.2 Detection and Surveillance

1. The system should produce hardware maintenance logs containing, as a minimum, records of:

- machine checks,
- instruction or command retries,
- data transfer retries,
- abnormal environmental conditions,
- power fluctuations/failures, and
- any other error conditions.

2. Ensure systems detect and react appropriately to secondary storage device errors. Such action should include recording the event.

5.3 Hardware Maintenance and Support

5.3.1 Routine Maintenance

1. Arrange for contracted maintenance personnel with access to equipment processing classified or designated information to be supervised by someone responsible to the department with sufficient background, training or qualifications to understand the risks associated with the work being done and provide assurance that only authorized access to sensitive information or assets takes place.

2. Ensure only trained TEMPEST maintenance personnel maintain TEMPEST-compliant equipment.

3. Document and implement procedures to ensure that each use of system remote link-up for manufacturer's technical support is specifically authorized.

4. Prevent unauthorized access to sensitive information when remote diagnostic access is required.

5. Document and implement procedures for hardware maintenance, consistent with the manufacturer's recommendations. Review these procedures annually.

6. Retain records of all hardware maintenance activity for a minimum of one year.

5.3.2 Problem Resolution

1. Develop, document and implement procedures for reporting, recording, tracking and resolving hardware problems.

2. Immediately report hardware problems affecting security to the IT security coordinator.

3. Maintain a contact list identifying operations, field services, software services, and data communications personnel.

4. Report all hardware equipment faults, logged manually or by the system, to the attention of both the staff responsible for the operation of the system and the equipment maintenance staff.

5. Where availability is a concern, develop and document escalation procedures, specifying problem priorities, actions to be followed and conditions for escalation.

6. Maintain records of all hardware equipment faults and the action taken to resolve them. Retain these records for one year.

5.4 Quality Assurance

5.4.1 Support Facility

1. Where availability is a concern, install alternate power sources to ensure the availability requirements are met.

2. Where data integrity is a concern, provide a stable power source and ground facilities consistent with the manufacturer's specifications e.g. an uninterruptible power supply (UPS) facility or power distribution unit which provides monitoring and clean, stable power.

3. Check system input power and grounding at least annually to ensure they meet the manufacturer's specifications.

4. Where a UPS is used, power through the UPS all hardware devices required for continued operation, e.g. remote terminal servers, remote printers, air conditioning for hardware operation, heating for cooling tower, lights. Consideration should also be given to emergency environmental facilities in the support and user areas.

Note: The UPS should shut off power to the system (file server or small system) in the event of fire or conditions exceeding specified environmental requirements.

5.4.2 Change Control

1. Assign and document responsibility for all aspects of change control functions, including:

- maintenance activities,
- configuration changes,
- equipment modifications, and
- micro code modifications.

2. Ensure all hardware modifications, maintenance activities and physical re-configurations are authorized.

3. Review additions, deletions or alterations to an existing system to ensure that the intended security profile of the system is not compromised.

4. Centrally control and document all changes to hardware equipment.

5. Retain the following documentation on site:

   - specifications,
   - current manuals,
   - log records, and
   - revision levels.

6. COMMUNICATIONS SECURITY

6.1 Administration

6.1.1 General

1. Centrally control, authorize and document the assignment of network access privileges, proxy accounts and default network accounts for all network users.

2. Conduct an annual communications security audit to review the implementation and effectiveness of the security features and access controls to systems and data resources.

3. Conduct a TRA of the department's total communications network, including system interconnections, communications components and the network itself.

4. Ensure communications systems features that address confidentiality, integrity and availability requirements meet the requirements of the application, e.g., authentication, error detection and correction, and alternate routing.

6.1.2 Separation of Duties

1. Where possible, separate the following communications duties:

- programming,
- operations,
- maintenance,
- software changes,
- hardware changes, and
- network changes.

6.1.3 Contracting

1. Ensure contracts specify the security requirements which apply to the communications equipment, network and related services controlled by a contractor. Contracts should be reviewed annually to reflect changes in requirements, and as a minimum, should address the following areas:

- release of information by the department:
  - need-to-know principle;

- release of information by the contractor:

- configuration details;
- information flowing in the network;

- protection of data:
  - disposal techniques for recorded network information;
  - procedures for line monitoring, maintenance, problem resolution, configuration control and change control;
  - TEMPEST or encryption requirements;
  - transportation of COMSEC documents; and

- required service levels:
  - define maintenance windows;
  - identify critical circuits;
  - define contingency plans.

2. Include in communications contracts a communications configuration chart and all design changes agreed upon between the department and contractor.

3. Ensure any configuration changes made during the period of the contract do not reduce the level of security provided to the classified, designated, or otherwise valuable information to be transmitted or received.

4. Ensure any configuration changes made during the period of the contract are reported, reviewed and approved, in a manner that is consistent with the communications change control process, prior to implementation.

6.1.4 Inventory

1. Assign and document responsibility for the maintenance of communications inventory records.

2. Maintain a current communications inventory and review it at least annually. Documentation should indicate whether an item is owned, rented or leased and the date of the last change. The inventory should identify:

- communications hardware and services, including:
  - circuits, lines or connections assigned, including the identification of the supplier;
  - the location of the physical termination of the circuits and lines;
  - media used (e.g. coaxial, fibre, unshielded twisted pair);
  - the circuit or line status (assigned or available);
  - the level of security classification or designation of each circuit or

line;
- hardware identifiers of remote input/output units;
- communications hardware (document model number and serial number), e.g., modems, dial-ins, concentrators, packet switched devices, encryption devices, and data switches;

- communications software and data, including:
  - software programs,
  - configuration database and files (libraries),
  - software procedures (e.g., Command Files),
  - software utilities,
  - security-relevant components,
  - licence numbers, and

- communications networks, including:
  - devices, e.g., servers, routers, gateways, bridges;
  - protocol and level;
  - network operating systems and applications software;
  - network media and transmission methods;
  - identification of node names (document: name, network address, type, location, responsible manager); and
  - security-relevant network applications, features and items.

3. Inventory records for each communications software item should include the following:

- security classification or designation;
- whether or not the item is considered privileged or powerful;
- the quantity and their locations;
- identification of owner, custodian, authorized user and maintainer; and
- date created or modified and version/level number.

4. Identify communications terminations and/or circuits by labels affixed on or near the equipment or on a diagram kept near the equipment. Cables should be labelled with unique identifiers.

5. Ensure that inventory items which are necessary for, or could affect, the system's protective mechanisms are assigned a security classification or designation commensurate with the most sensitive information or assets processed or transmitted by the system.

6.1.5 Departmental Standards

1. Assign and document responsibility for departmental communications standards.

2. Ensure that departmental communications standards are documented, maintained, reviewed annually and marked with an issue date.

3. Where departmental communications standards are not followed as specified, the differences should be documented, including:

- cable pin configurations (show pinouts and colour coding);
- circuit/line options;
- labelling conventions:
  - speed;
  - parity;
  - asynchronous or synchronous;
  - character length;
  - data communicating equipment (DCE) or data terminating equipment (DTE);
  - number of logical links;
  - protocol level;
- line cards/units:
  - jumper options;
  - programmable read-only memory (PROM) levels noting any special options;
- soft options used in intelligent network nodes, data switches, multiplexors, local area networks, etc.:
  - various options chosen for each unit model;
  - any critical parameters;
  - closed user groups;
  - classes of devices; and
- manufacturer's specifications and user documentation.

4. Keep a current copy of the departmental communications standard at an off-site location.

6.1.6 Configuration

1. Maintain a chart of the current IT communications configurations, review it at least annually and mark it with an issue date.

2. Ensure the communications configuration chart includes hardware components and classes of interconnections used to establish, maintain and terminate communications. In addition, configuration charts should highlight exceptions to a departmental

communications standard.

3. This chart should describe any special status and/or protection requirements, e.g., control terminals and access privileges associated with lines and circuits. Where this information is deemed sensitive, mark the chart with the appropriate designation or classification level.

4. Where availability is a concern, identify and document the minimum configuration to support critical applications and review it at least annually.

5. Keep a current copy of the configuration (both operational and critical minimum) at an off-site location.

6.2 Communications Maintenance and Support

6.2.1 Routine Maintenance

1. Assign responsibility for all maintenance activity.

2. Where access to classified or designated information is possible, arrange for contracted maintenance personnel to be supervised by someone responsible to the department with enough background, training or qualifications to understand the risks associated with the work being done and provide assurance that only authorized access to sensitive information or assets takes place.

3. Retain records of all communications maintenance activity for one year.

4. Authorize and control the use of communications test equipment, network diagnostics-monitoring tools, and privileged and powerful communications software utilities.

5. Use approved techniques to sanitize or dispose of communications-monitoring recordings. These techniques are described in the Operations Security chapter.

6.2.2 Problem Resolution

1. Develop, document and implement procedures for reporting, recording, tracking and resolving communications problems.

2. Retain records of problems and their resolutions for one year.

3. Immediately report communications problems affecting security to the IT security coordinator.

4. Maintain a contact list identifying communications support personnel, field service personnel, communications software services personnel, data communications vendors and telecom carriers.

5. Where availability is a concern, develop and document escalation procedures, specifying problem priorities, actions to be followed and conditions for escalation.

6.2.3 Change Control

1. Assign and document responsibility for all aspects of change control functions, including:

- maintenance activities,
- configuration changes,
- equipment modifications, and
- software changes.

2. Do not make changes to cryptographic equipment without prior approval of the departmental COMSEC authority.

3. Centrally control and document all changes to communications equipment, communications software and network configurations.

4. Retain on site the following documentation with respect to modifications:

- specifications,
- updated manuals,
- configuration charts, and
- log records.

5. Review additions, deletions or alterations to an existing system to ensure that the security profile of the system is not compromised.

6.2.4 Operational and Control Procedures

1. Develop, document and implement procedures governing the communications operations environment including multiple systems or networks. Include the following:

- communications start-up;
- communications shut-down;
- equipment operation;
- enabling/disabling/switching specific communications links/lines/ports;
- backup procedures/requirements, e.g. configuration data and software;
- maintenance;
- handling of sensitive material;
- emergency situations;
- communications logs review;
- the use of network performance monitoring and reporting; and
- the use of network management systems utilities.

2. Ensure communications equipment, excluding user terminals, is operated only by authorized personnel.

3. Where multiple systems or multiple networks are involved, develop, document and implement centralized policy and procedures for the network interconnection. Include the following:

- assignment of a centralized network coordinator,
- configuration and change control guidelines,
- network performance monitoring and reporting,
- network security policy and procedures,
- network applications,
- problem reporting and escalation, and
- technical support.

6.2.5 Detection and Surveillance

1. Monitor communications facilities for discrepancies such as:

- protocol errors;
- inconsistent communications identification data as related to hardware identification and polling responses;
- sequence errors;
- status and error alarms;
- data inconsistencies;

- communications access control errors; and
- errors in network applications, e.g., E-mail, Electronic Data Interchange (EDI), file transfer, proxy accounts, routing.

2. Conduct periodic tests of security features to ensure communications controls have not been compromised or misused. Record the results of these tests for audit and quality assurance purposes.

3. Where integrity of information is of concern, (e.g., funds transfer) keep records to ensure accountability of information throughout the communications system network, including intermediate locations, such as nodes, concentrators, network monitors, front ends, switches, gateways and routers.

4. Retain security logs, documents and records for one year.

5. Keep change control records for a minimum of one year for problem and security-incident analysis.

6.2.6 Prevention

1. Systems should be capable of recognizing active communication links with users, so that links can be disconnected in response to recognized incidents or in order to reconfigure systems.

6.3 Communications Software

1. Where a department develops communications software, all software criteria documented in Chapter 7, Software Security, apply.

6.4 Protection of Information in the Communications Environment

6.4.1 General

1. Obtain direction and guidance for COMSEC from the departmental COMSEC authority.

2. Where encryption is required, the departmental COMSEC authority will select the encryption technique. (e.g., digital signatures, public key cryptography, approved cryptography.)

3. Obtain keying material for encryption devices from the COMSEC authority.

4. Handle, store, use, protect and account for keying material for encryption devices in accordance with COMSEC procedures.

5. Encrypt passwords and other security-related information.

6.4.2 Designated Information

1. Protect the transmission of all extremely sensitive designated information (Protected C) by approved cryptography or other approved COMSEC measures.

2. Where supported by a TRA, protect other sensitive designated information (Protected A and B) by controlled communications measures and/or other COMSEC measures, such as:

- dedicated circuit;
- line encryption;
- firewall;
- hardware identifier in the terminal;
- external communications access control devices, e.g. smart cards, tokens;
- Closed User Group; and
- dial connection initiated by the host site.

3. Use TEMPEST methodology to protect data which is not classified, but, as determined by a TRA, warrants protection against disclosure through compromising emanations.

4. Where cryptography is employed, ensure the equipment is operated and maintained only by trained, authorized and appropriately-cleared personnel.

6.4.3 Classified Information

1. Protect the transmission of all classified information by approved cryptography or other approved COMSEC measures.

2. Install, operate, maintain and protect communications systems processing classified information in accordance with appropriate COMSEC Manuals (CID 01/8, CID 01/10, CID 09/7A and operation doctrines).

3. Where warranted by a TRA, use TEMPEST-compliant equipment or other

approved methods to protect against compromising emanations, for telecommunications or electronic processing or storing classified information.

4. Where steps have been taken to protect against compromising emanations, the COMSEC authority shall ensure periodic tests and/or inspections are conducted to confirm the continuing integrity of the emanation protective measures.

5. Where there is a change in the sensitivity/classification of information being processed, stored or transmitted, or a change in the TRA affecting TEMPEST-compliant measures, the COMSEC authority shall review the existing compromising-emanation protective measures to ensure their adequacy.

6. Where cryptography is employed, ensure the equipment is operated and maintained only by trained, authorized and appropriately-cleared personnel.

7. SOFTWARE SECURITY

7.1 Administration

7.1.1 Separation of Duties

1. To the degree practical, assign the following functions to different individuals in separate organizational entities:

- systems programming,
- systems administration,
- database administration,
- application programming,
- quality assurance and acceptance testing, and
- program library maintenance and control.

7.1.2 Inventory

1. Assign and document responsibility for the maintenance of software inventory records.

2. Maintain inventory records for production software and data assets. Inventory items should include:

- systems software,
- database software,
- application software,
- access control software,
- software utilities,
- software procedures and command files,
- program and procedure libraries and directories,
- databases and data files, and
- operational configuration parameters.

3. Inventory records for each item should indicate:

- security classification or designation;
- whether the item is considered privileged or powerful software;
- warranty/maintenance conditions;
- the number of copies or valid users along with their physical locations;
- the owner, custodian, authorized user and maintainer; and
- a creation/modification date, version/level number and any special

modifications.

4. Ensure that inventory items providing or affecting the protective mechanisms of the system are assigned a security classification or designation, commensurate with the most sensitive information or assets on the system.

7.1.3 Security Review

1. Authorize, monitor and review the use of privileged or powerful software.

2. Conduct an annual security review of software items and data. The review should include:

- change control practices and procedures,
- compliance with documentation standards,
- operating system and application program library controls,
- the effectiveness of logical access controls,
- controls for the use of privileged or powerful software,
- integrity and availability controls,
- software and data-related aspects of contingency measures, and
- accuracy of inventory.

7.2 Design, Development, Maintenance, Quality Assurance and Acceptance Testing

7.2.1 System Development Life Cycle Standards

1. Document and implement software acquisition procedures to establish and maintain a level of confidence appropriate to the sensitivity of the information to be stored or processed.

2. Document and implement procedures, often referred to as the System Development Life Cycle (SDLC), to guide and control the design, development, approval, test, documentation, implementation, maintenance and protection of production software and data items.

3. The SDLC should include the following phases:

- preliminary analysis or feasibility study,
- systems analysis,
- general design,
- detail design,
- development,

- quality assurance and acceptance testing,
- implementation, and
- post-implementation maintenance and review.

4. Ensure the SDLC includes documented provisions, limitations and required authorizations for bypassing one or more of the established phases.

5. Review the security requirements for compliance with IT security standards and statements of sensitivity and have the review signed off by an appropriate authority during each phase of the SDLC.

6. The IT security coordinator(s) should participate in all phases of the SDLC and the security requirements review process.

7. For systems with high integrity concerns, the appropriate auditors should be included in the security requirements review process.

7.2.2 Change Control

1. Assign and document responsibility for maintaining change control records.

2. Document and implement procedures for controlling changes to production software. The change control procedures should include the mechanisms for:

- requesting changes,
- recording and tracking outstanding requests,
- approving requests,
- testing and documenting changes, and
- incorporating changes.

3. Where possible, maintain production software in both source and executable form. Production software includes:

- operating systems and supporting utilities,
- database management systems,
- application software,
- access control software, and
- operational parameters.

4. Where possible, acquire and maintain third party proprietary or custom-developed software in both source and executable form.

7.2.3 Problem Reporting

1. Assign and document responsibility for maintaining and tracking problem reports.

2. Document and implement procedures for the reporting, monitoring, and resolution of software and data discrepancies. As a minimum, record date, time and nature of the problem.

3. Immediately report to the IT security coordinator software or data problems which could affect security.

4. Give priority to the resolution of software and data problems that affect security.

7.2.4 Software Library Control

1. Assign and document responsibilities for software library maintenance and control, which include:

- custody;
- access control for production, audit, and change control purposes;
- onsite and offsite backups; and
- maintenance of the records of access and changes.

2. Document and implement software library backup procedures to provide the capability of restoring specific versions of software elements.

3. Restrict update privileges to individuals responsible for:

- software development, in the case of development program libraries;
- quality assurance and acceptance testing, in the case of acceptance testing libraries; and
- transferring software to production status, in the case of production libraries.

4. Document and implement software management and distribution procedures for distributed and remote systems to ensure:

- all software distribution is authorized;
- licensing agreements concerning usage and disposal are observed; and
- software and data are backed up and updated in a consistent and controlled manner.

7.2.5 Quality Assurance and Acceptance Testing

1. Assign and document responsibilities for quality assurance functions including:

   - development and implementation of acceptance test standards and criteria,
   - performance of quality assurance and acceptance testing,
   - reviewing and reporting on these test results to ensure established test criteria are met prior to implementation, and
   - custody and retention of test results.

2. Production data should not be used for testing purposes. When it is not feasible to create test data, copies of production data may be used provided the confidentiality requirements of the production data are satisfied.

3. Software should be tested in an environment separate from the production system.

4. Where security concerns warrant, testing should include:

   - line-by-line code reviews, and
   - comparison checks of executable routines.

5. When software is transferred to acceptance testing or production status, re-compile/re-assemble the transferred source code, if available, within the recipient libraries to ensure compatibility between source and executable code.

6. Where practical, examine all software for malicious codes.

7.3 System Software

7.3.1 Configuration

1. Based on configuration and security requirements, establish and document parameters and options required to start up the operating system, supporting utilities, third party proprietary and custom software products.

7.3.2 Identification

1. Systems should have the capability of identifying discrete elements including:

   - users,
   - data,
   - media,
   - software programs,
   - hardware components, and
   - communication links.

2. When data is written on removable media, use the system capabilities for writing and verifying machine-readable labels.

3. Use system capabilities to verify the identity of volumes and files recorded on machine-readable labels or file systems against information contained in access requests.

7.3.3 Isolation

1. Obscure passwords or similar authenticators by one-way encryption.

2. To restrict access to system and data resources in a multi-user environment, implement operating systems and access control systems with an evaluated level of trust appropriate to the sensitivity of the data.

3. Where users have different duties and access rights, restrict users to specific required functions by implementing controls, such as restricted transaction processing or captive accounts.

4. To provide for user-user and user-computer system isolation in a multi-user environment, restrict and monitor the following privileges:

   - changing computer system privileges or controls,
   - changing protective features or parameters affecting another user,
   - halting the computer system,
   - allocating system and data resources for personal use, and
   - inhibiting the allocation and sharing of system and data resources.

5. Where confidentiality is a concern and users do not share a common need-to-know, obscure the contents of erasable media using an approved technique at the time the file space is released for reuse or destruction.

6. Ensure the system automatically terminates or re-authenticates an interactive user's session after a predefined period of inactivity.

7. Where confidentiality is a concern, ensure display screens and all associated memory are cleared upon user sign-off or after a predefined period of inactivity.

8. Ensure systems inhibit or overwrite authentication information on display screens.

9. Do not include user authentication information on any form of computer output.

7.3.4 Access Control

1. Based on requirements documented in system statements of sensitivity, implement an access control system to control and monitor access to the system and data resources.

2. At each successful sign-on, the user should be informed of the date and time of the last successful sign-on and any subsequent failed sign-on attempts.

.

3. Ensure access control mechanisms control access to system and data resources and are based upon the user's identity, functional requirements and pre-defined authorization. User privileges could be restricted by:

- controlling user read, write, create, delete and execute capabilities;
- implementing access control lists;
- implementing capability lists; and
- controlling hierarchical authorization such as owner, group, system and universe.

4. When access to system and data resources is denied, do not provide an indication of the specific reason for denial.

7.3.5 Integrity

1. Design recovery routines and procedures to minimize the possibility of mis-routing interrupted transactions or transmissions.

2. Where changes of processing state are required, document and implement procedures to ensure the integrity of the operating system and supporting software which are used to process classified information.

7.3.6 Availability

1. For systems with critical availability requirements:

   - use redundant hardware, software and communications to process the transactions simultaneously;
   - use hardware and/or software techniques to detect hardware/software failures in the primary and backup systems;
   - ensure the backup system automatically switches the required hardware, software and communications equipment to primary status upon failure of the primary system; and
   - ensure the application software program processing the transactions on the primary system are logically different from the backup system.

7.3.7 Surveillance

1. Test the system's surveillance and protective mechanisms at least annually, or following changes to security-relevant software, to ensure continued capability of the system to prevent unauthorized:

   - access to system and data resources;
   - access to residual data;
   - use of privileged capabilities; and
   - read or write from outside allocated memory bounds.

2. Ensure the system records security-relevant events, including:

   - job or process status (entry, initiation, completion, deletion, restart, and abort);
   - file, volume, and database accesses (open, close, create, delete, rename);
   - communications device connect, disconnect and re-configuration;
   - network status messages;
   - user sign-on and sign-off;
   - system operator commands and responses;
   - system and subsystem status messages (start-up, shutdown, abort);
   - system-generated messages or requests regarding configuration changes;
   - changes to system logging facility status (start, stop, alter, print, dump, delete, rename and overflow);
   - changes to access control information;
   - changes to lists of authorized users;
   - detected security incidents; and
   - use of privileged or powerful software.

3. For each security event, record the following information, if applicable:

- nature and type of incident,
- date and time,
- user identification,
- device identification,
- job or process identification,
- identification of resource accessed,
- mode of access, and
- configuration details.

4. When logging security-relevant information whose confidentiality must be protected based on the need-to-know principle, specify only that a particular type of event has occurred.

5. Where log records are machine-readable and of sufficient volume to make manual recognition of security-relevant events impractical, use software routines to highlight security-relevant events.

6. Ensure that, when a security-related event is detected, a highlighted message is routed to a system console or printer for further analysis.

7. Ensure that, when a severe security-related event is detected, an audible or visual alarm is immediately activated.

7.4 Data and Database Administration

1. Assign and document responsibilities for data and database administration including:

- access control,
- data dictionary,
- definition and creation,
- integrity and audit, and
- backup and recovery.

2. Ensure the implementation of the database maintains isolation of information based on sensitivity and the need-to-know principle.

3. Conduct database audit checks to verify the logical and physical consistency of the database and identify discrepancies such as lost records, open chains and incomplete sets.

4. Use a data dictionary to document, standardize and control the naming and use of data.

5. Restrict and monitor the use of database maintenance utilities that bypass access controls as these utilities are considered to be privileged and powerful software.

6. The system should be capable of automatically recovering the database following a system or application software failure.

7. Where availability is critical, maintain duplicate databases on separate physical devices and perform all database maintenance transactions simultaneously on both databases.

8. Where confidentiality is a concern, automated or manual controls should be implemented to protect against unauthorized disclosure by means of inference search techniques.

9. Where the integrity of records stored on the database is a concern, implement data integrity verification techniques, such as message and record authentication coding or hash total techniques.

10. Where the auditability and authorization of records stored on the database is a concern, ensure:

- the user identification and authentication process positively identifies the authorizer;
- the user identification of the authorizer and data entry person is retained on the transaction record; and
- all critical data elements, including transaction date and time, authorizer and data entry user identifiers, are included in the data integrity verification process.

7.5 Applications Software

7.5.1 Identification

1. Where differing access privileges exist within an application, ensure users are uniquely identified.

2. Application access control mechanisms should use the user identification obtained by the system during initial sign-on, rather than an alternate or subsequently obtained identifier.

3. Use a standard naming convention for applications, programs, databases, files and

data elements to facilitate the identification of software assets.

7.5.2 Isolation

1. Where differing access privileges exist within an application, restrict users in their view of the data, through use of:

- the captive user concept; or
- data file, record, and element protection.

7.5.3 Access Control

1. Where differing access privileges exist within an application, implement access control mechanisms to restrict access to application and data resources in accordance with users' functional requirements and authorization.

7.5.4 Integrity

1. For systems with high integrity requirements:

- test the application's protective mechanisms following changes to security-relevant software;
- ensure applications incorporate checks to ensure the validity and correctness of input data or parameters (such as edit routines, range/reasonableness checks, batch totals, sequence numbers, check-sums, hash totals, error-correcting codes);
- design the system to ensure that data can be recovered automatically or with the assistance of the data originator following computer crashes;
- design the system to include backup requirements to ensure data can be fully recovered, taking into account the length of time an error may remain undetected;
- immediately transmit a copy of each processed transaction to be stored at an off-site location;
- design the system to ensure that the process output is checked against control records (such as batch totals, record/block counts, check-sums,

hash totals, sequence checks);
- output control records at intervals during the process and review them prior to acceptance of the process output; and
- acknowledge receipt of information from the output process.

7.5.5 Surveillance

1. Where auditability of access to sensitive information is a concern, the system or application logs should include the contents of the data accessed by the user as well as the identification of the recipient.

7.5.6 Fourth-Generation Languages

1. Ensure controls are in place to protect the confidentiality, integrity and availability requirements of the system from compromise through the use of a fourth-generation language. Controls include:

- restricting access to production data and resources;
- logging and monitoring access to production data and resources; and
- limiting system resource consumption, such as processing time and the number of database reads or writes.

2. Develop and test in a separate environment all fourth-generation language programs which modify data.

8. OPERATIONS SECURITY

.

8.1 Administration

8.1.1 Separation of Duties

1. Prohibit operations personnel from making changes to computer programs (executable and control code) without authorization.

2. Ensure operations personnel do not make, and are not responsible for, input additions or error corrections to production data unless documented policy has been issued outlining the circumstances under which these actions will be permitted and the audit controls which will apply.

3. Ensure hardware, excluding user workstations, being used in the production process is operated only by operations personnel. In an emergency situation, non-operations personnel may operate hardware under the direct supervision of operations personnel.

4. When a data control function is established, it should consist of a separately staffed unit whose duties are designed to provide separation between users and operations personnel. In certain circumstances, further separation of duties within the data control function may be required.

5. Prohibit operations personnel from initiating their own jobs without prior authorization.

6. Departments should, for control purposes, ensure there is a rotation of operators on sensitive applications.

8.1.2 Mode of Operation

1. In all instances where classified or designated information is processed in either public or private sector facilities, choose and specify the mode of operation in accordance with Chapter 1 of this document. Use the specified mode of operation in the TRA process for determining appropriate safeguards.

2. When it is necessary to change the mode of operation and confidentiality is a concern, take the following precautions:

- disconnect all communications lines which do not comply with the requirements of the mode of operation to be used;
- sanitize the memory;

- disconnect any access path to data which is not specifically required to support processing of the new mode of operation;
- use a fresh copy of an appropriately-protected version of the operating system for the new system; and
- use an approved means to obscure the contents of all erasable media to be shared by the system.

3. When a remote system is unable to support the local mode of operation, ensure the local system disables the communications link between them.

8.2 System Access and Authorization

1. Ensure computing facilities are used only for authorized work.

2. Ensure no access to IT systems and data is permitted without the user being uniquely identified. A user identifier by itself should not grant access privileges.

3. Ensure user identifiers are designed to permit group level identification of individuals who have the same:

- level of security-screening;
- need to access the IT systems and data; and
- functional requirements.

4. Develop and implement procedures for the preparation, issue, change, cancellation and audit of user identifiers.

5. Deny access to system or data resources until the individual's identity has been authenticated, and authorized privileges have been confirmed, automatically or manually.

6. Where the authentication process uses unique authentication codes or passwords, ensure such items are:

- generated, controlled and distributed in a manner which maintains the confidentiality and integrity of the authentication code;
- known only to the authorized user of the account;
- pseudo-random in nature or verified by an automated process designed to counter triviality and repetition;
- at least six characters in length;
- one-way encrypted;
- excluded from unprotected automatic log-on processes; and
- changed in accordance with the following minimum schedule:

Top Secret	- Monthly
Secret	- Quarterly
Confidential	- Quarterly
Protected	- Biannually
Other	- Biannually

7. In addition, where the accounts are considered to be privileged or restricted system or data resources, ensure that authentication codes or passwords are:

- at least eight characters in length, and
- changed at least monthly.

8. Ensure records concerning system authentication mechanisms, codes or passwords used to authenticate identities are provided the same level of protection as that required by the sensitivity of data processed.

9. Obtain authorization whenever a security feature normally used on the system cannot or will not be used. Document the actions taken in these circumstances and report them as a security incident.

10. Control workstations which have privileges over and above those of other devices on the system to ensure their use is authorized and audited.

8.3 Procedures and Controls

8.3.1 Operating Procedures

1. Procedures governing the day-to-day functions of the operating environment are required and should cover, as a minimum:

- power up/power down sequence,
- start up/shut down of systems (including operating system and applications),
- equipment operation,
- trouble reporting,
- security incident handling,
- operator-performed maintenance,
- operator commands,
- operator responses to systems and application program-generated messages,
- start and stop communications,
- backup and restore,
- sanitizing the system,

- sanitizing erasable media,
- disposal of unserviceable erasable media,
- emergency situations,
- shift hand-over,
- over-riding of security controls,
- recovery/restart,
- handling of classified/designated material,
- environmental support equipment, and
- setting and resetting the system clock.

2. Ensure that all software requiring operator response is accompanied by pertinent operator procedures and training before being accepted into the production environment.

3. Develop and implement verification procedures for the backup process, e.g., a compare or restore, to ensure the backup was successful.

4. Maintain sufficient generations (as dictated by the application's data retention requirements) of backup data to ensure that data can be recovered.

5. Ensure shift hand-over procedures maintain operational continuity and include a shift overlap, where possible.

6. Develop and implement procedures to control the overriding of system security including authorization, control, audit and return to use of the security feature.

7. Develop and implement procedures to cover the transfer of the operational control of the hardware and software environment from the normal operations group to any other person or group such as system maintenance personnel. Include actions which minimize the possibility of any compromise of the confidentiality, integrity and availability requirements of the system and data resources.

8. When machine-readable labels are used on media, prohibit bypassing the label except for specific circumstances supported by written authorization.

9. When machine-readable labels are used and bypassing label processing is authorized, mechanisms or procedures should be in place to ensure that the correct volume is mounted.

10. Provide accountability and control for sensitive, pre-printed and computer-generated forms from the time of receipt or production until they leave the IT environment. Examples of these forms are visas, passports, cheques and warrants.

8.3.2 Input and Output Controls

1. When confidentiality or integrity of output is a concern, take actions to ensure that:

- jobs are only rerun or reprinted under strict controls and with prior authorization;
- output is delivered only to the owner or to a person who has been authorized to receive it; and
- receipts are obtained when output is delivered.

Integrity

1. Develop procedures to ensure the accountability of data being input to a system. These procedures should include measures to provide accountability for:

- input materials received by operational units; and
- transactions or other data being input to the system locally or remotely.

2. An audit trail of transactions being input to a system should relate each specific transaction to the individual who entered it.

Note: This requires the identification of individuals using data entry devices and records that show who entered which transaction. Identification of the individual may be by means of logical identifiers unless the probability of deliberate attempts to compromise the transactions is deemed to be high, in which case physical identification is required.

3. When data verification is performed, it should be done by an individual other than the person entering the data.

4. When only soft copy authorization records are maintained, ensure that the logs containing details of transactions are maintained and safeguarded.

Confidentiality

1. Take actions to ensure that:

- only the number of copies of output specified by the person generating the output is produced;
- distribution of all output is logged;
- unless sensitive information is deleted from a system dump, the dump is protected commensurate with the highest level of information on the system until it is destroyed or disposed of; and
- the appropriate security classification or designation is marked on all

output.

2. Position remote hard copy or display devices to prevent observation by unauthorized personnel.

8.3.3 Detection and Surveillance

1. Keep records identifying each individual in the operations area. Scheduled operations personnel are required, as a minimum, to sign in at the beginning, and out at the end, of each shift.

2. System logs should be checked at randomly selected intervals to verify that all processing was authorized.

3. System logs should be reviewed to determine if the authorized number of licences is being exceeded or if unauthorized software is in use.

4. The IT security coordinator, or another person designated by the department, is responsible for the regular review of security logs and records to ensure that all responses to security incidents are correct and comply with existing procedures.

5. IT facilities should produce a report on the type and frequency of errors. The IT security coordinator or designate should review information in this report for security connotations.

6. Review and analyse all operator errors for security implications.

7. Hard copy logs and records that are used for accountability or control purposes should be designed so that the removal of records can be detected (e.g., paper log pages could be sequence numbered).

8. Retain, for at least one year, security logs, records and documents used for accountability or control purposes.

9. Protect logs and security records commensurate with the highest level of classification/designation of information on the system.

8.4 Media

8.4.1 General

1. Assign responsibility for the control and care of all removable media.

2. Develop and implement procedures for the handling, protection and accountability

for all removable media entering, remaining within and leaving the IT environment.

3. Undertake regular and proper maintenance of erasable media.

4. Where controlled access is a concern, information of different sensitivities should be maintained on separate physical devices to maintain isolation.

8.4.2 Media Library

1. Restrict media-library access to authorized personnel, and log and audit all access.

2. Records generated for accountability of IT media should include :

- media identifier,
- identification of owner,
- date and time of transaction, and
- details of transaction including appropriate authorization.

3. Unless an automated media management system verifies ownership, ensure all write-protection mechanisms are enabled for media containing information to be retained when the media is removed from the drive.

4. Ensure media write-protection mechanisms are disabled only by IT staff assigned responsibility for the control and care of removable media

5. Develop and implement procedures to allow sensitive removable IT media to be securely stored and used only with written authorization.

6. Ensure IT media is not removed from the operations environment without the approval of a third party, specifically designated by the department.

7. When removable media is stored in off-site locations, ensure controls are commensurate with the sensitivity of information contained on the media.

8.4.3 Inventory

1. Take an inventory of all removable IT media under the control of the media library in accordance with the following minimum schedule:

- Top Secret - Monthly
- Secret - Quarterly
- Confidential - Quarterly
- Protected - Annually

- Other - Annually

2. Immediately inform the IT security coordinator of any discrepancy between the records pertaining to removable media and the authorized disposition of such media.

3. The inventory of removable media should be taken by a minimum of two individuals working together, one of them employed in an area independent of the media library function.

8.4.4 Identification

1. Develop and implement procedures to ensure that the identity of volumes and files of removable media is verified against the information contained in requests for access.

2. Procedures should be developed and implemented to ensure that all removable media contains machine-readable internal labels.

3. To verify the identity of the media, machine-readable labels should be read by the system when the media is mounted.

8.4.5 Markings

1. Assign IT media a security classification or designation commensurate with the most sensitive information on the media.

2. Clearly mark the security classification/designation on all IT media in accordance with Appendix OPS-I.

Note: When every piece of IT media in a facility has an identical security classification or designation, the classification/designation level need be marked only when the media leaves the IT facility.

3. When removable IT media is to be removed from the IT environment, clearly indicate ownership in eye-readable form on the media itself and on the containers used for such media.

4. Ensure all media used to back up information owned or received by the department is government-owned.

8.4.6 Disposal/Re-use

1. Where confidentiality is a concern, ensure that, before being released from the IT environment, erasable media previously used to store classified/designated information is

sanitized using an approved erasure technique. Examples of such approved techniques are contained in Appendix OPS-II.

2. Remove markings from erasable media and containers only after verification of the sanitization procedure.

3. When equipment containing media is to be removed from the IT environment for servicing, apply the techniques listed in Appendix OPS-II.

4. Where confidentiality is a concern, use an approved technique listed in Appendix OPS-III to erase or overwrite erasable media that contains sensitive information and is to be retained for re-use or re-allocation within the same environment.

5. Where confidentiality is a concern, procedures for securing materials used to produce sensitive output, such as printer ribbons, OPC cartridges, carbon paper, and mylar film, should be developed and implemented, to ensure these materials are:

- physically secured during silent hours,
- controlled when the output device is left unattended,
- disposed of in an approved manner (e.g. by burning or shredding), and
- suitably protected, including inventory control, while awaiting destruction

8.5 Contingency Measures

1. Store at an off-site location current copies of all critical operational data and material and a sufficient supply of the critical media resources to ensure the continued provision of the minimum essential level of service, as defined in the department's business resumption plan. These items should include:

- operating system software,
- configuration diagrams/charts,

- utilities,
- applications system software,
- data,
- documentation,
- encryption keys,
- an up-to-date telephone number contact list,
- passwords, and
- forms.

2. Store, at the off-site location, an index of resources containing:
   - identification of the resources and data,
   - names of the owners of the data, and
   - the classification or designation of the data.

3. Review the operational requirements of the department's contingency plan at least annually, to ensure that all critical operational components, materials and resources have been identified.

4. Maintain backup media and associated documentation consistent with contingency plan requirements both on site and off site.

5. Ensure an up-to-date list of telephone numbers to be used in responding to contingencies and emergencies is readily available to operations personnel.

CLASSIFICATION/DESIGNATION MARKING ON MEDIA OR DISPLAYS

1. General

The following colour codes may be used to assist in denoting the security classification or designation of information within an IT facility:

CLASSIFICATION / DESIGNATION	COLOUR CODE
Top Secret	Orange
Secret	Red
Confidential	Green
Protected	Blue

2. Storage Media

Storage media includes all magnetic and non-magnetic media that is removable or not, for example, floppy disks, fixed hard disk drives, optical platters, CD ROMs, smart cards, and magnetic tapes (cassettes or reels).

Place the sensitivity marking on the media protective cover in plain language and eye-readable form. In addition, where feasible, put similar markings directly on the media, for example on the casing of the DAT cassettes.

Note: Formats not covered above should be handled by extension or analogy.

3. Printed Output

Place the sensitivity marking on the top right corner of the individual sheet or segment of a roll as follows :

SENSITIVITY	FREQUENCY
Top Secret or Secret	every page
Confidential or Designated	cover sheet

Note: This can be done by program instruction, use of pre-printed stationery or manually.

Additional information on the control of printed output can be obtained from the *Treasury Board Manual*, Security volume, Chapter 2-1, Appendix D.

4. Display

Place the sensitivity marking in an eye-readable form that is continuously present on the display screen. In addition, place a warning on the display unit indicating the highest classification or designation of information for which the device is used.

Note: When every display unit has an identical security classification or designation, the classification/designation level need be marked only at the facility.

5. Computer - Output Micrographic (COM)

Microfilm	Plain language and eye-readable form on cartridges or cassettes.
	At the beginning and end of the film in plain language and eye-readable form.
	At the centre of the top and bottom of each individual frame.
Microfiche	Envelopes clearly marked in plain language and eye-readable form.
	On the header line in plain language and eye-readable form, along with the fiche number and total number of fiche (e.g. 1 of 5).
	At the centre of the top and bottom of each individual frame.

MEDIA SANITIZATION

1. Definitions

SANITIZATION — Erasing or overwriting magnetic media to ensure that information stored on the media is no longer retrievable.

DESTRUCTION — Subjecting the magnetic media to sufficient physical damage to ensure that none of the stored information is retrievable.

COERCIVITY — Coercivity of magnetic media refers to the magnetic field necessary to reduce a magnetically-saturated material's magnetization to zero.

DEGAUSSING UNITS — A device designed to generate a coercive magnetic force for the purpose of degaussing magnetic storage media so that the data is no longer retrievable.

MAGNETIC MEDIA TYPES — Type I products are used to degauss magnetic media whose coercivity is no greater than 350 Oersteds (Oe). Type II products are used to degauss magnetic media whose coercivity is between 350 Oe and 750 Oe. Type III degaussers have satisfied the requirements to degauss magnetic media having a maximum coercivity of up to 1700 Oe. Refer to the media manufacturer to determine the media type.

2. Sanitization Requirements

Where a sanitization procedure is not practical, or media other than listed below is a concern, advice should be requested from the RCMP, Technical Security Branch.

a) Non-removable magnetic media (disks and disk packs)

- One approved method used to declassify media is to write over every addressable location first with one pattern, usually binary “one” digits, and then with the complementary pattern, in this case, binary “zero” digits. This cycle of overwrite is then repeated alternately for a

minimum of three cycles. After the overwrite has been accomplished, unclassified random data should be written in all data locations on all tracks of the disk and left there.

The electrical current used in overwriting shall be at least equal to that used in recording the information and sufficient to override any peaks or valleys which may have occurred in the power source during the recording period. This overwrite current shall not be of such a strength as to damage or impair the equipment.

b) Removable magnetic media (tapes, cartridges, and disks)

- Pass through a bulk eraser or tape degausser which, in each case, has been approved for the media type and classification/designation.

c) Sanitization of Type I media using a permanent magnet:

- Expose the recording surface to a permanent magnet with a field strength of at least 1500 Oe at the recording surface;

- Wipe the entire surface at least three times by non-uniform motion of the magnet ensuring all tracks have been covered by the centre of the magnet.

Note: When using a magnet to erase the media, a thin sheet of clear plastic (from 1 to 5 mils) should be used to prevent damage to the recording surface of drums, disks and disk packs.

d) Magnetic memory

- Magnetic core memory - overwrite all addressable areas 1000 times with alternating 0 and 1 bits.

- EPROMS should be destroyed unless they are to be reprogrammed and reused within the same environment.

e) Optical media (disks and CD-ROM)

- Since no approved sanitization techniques exist, the media must be destroyed.

4. Destruction Methods

Destruction techniques must guarantee that the storage surfaces are completely destroyed. Examples of destruction methods are burning, emery wheels, crushing and shredding. Refer to "Physical and Environmental Security", TSSIT, Chapter 4.

Note:

For further clarification and information on media sanitization, refer to CSE - CTIB 19/87, “Guidelines for Clearing and Declassifying Automatic Data Processing Storage Devices”.

For further information on degaussers, refer to CSE, CTIB 7/96, “CSE Approved Degaussers for Erasure of Magnetic Media”.

RE-USE OF MEDIA IN THE SAME ENVIRONMENT WHERE CONFIDENTIALITY IS A CONCERN

NOTE: Media can be reused only for the same level of sensitivity or above.

1. Removable magnetic media (tapes, cartridges, and disks)

   - Overwrite once at the normal recording current level with a single alphanumeric character or bit pattern, or pass through an approved degausser or bulk eraser.

2. Non-removable magnetic media (drums, disks and disk packs)

   - Verify that the media drive is functioning correctly, then overwrite all storage areas once with the binary digit ONE or the binary digit ZERO at the normal recording current level.

3. When the capability exists as an integral part of the storage sub-system, prior to re-using or re-allocating erasable media, an AC/DC erase should be applied to all data tracks after the tracks have been overwritten and the overwrite verified.

4. EPROMS should be destroyed unless they are to be reprogrammed and reused within the same environment.

5. Any other technique approved by the RCMP.

REFERENCES

FEDERAL STATUTES

- *Access to Information Act*
- *Financial Administration Act*
- *Interim Policy Guide: Access to Information Act and the Privacy Act, Parts II and III*
- *Interpretation Act*
- *Official Secrets Act*
- *Privacy Act*
- *Public Service Employment Act*
- *Public Service Staff Relations Act*
- *Tenants Act*

RCMP PUBLICATIONS

- *Construction Specification for Secure Room C* (SSB/SG-23), March 1991
- *Construction Specification for Secure Room D* (SSB/SG-22), March 1991
- *Guide to Preparation of Physical Security Briefs* (SSB/SG-25), October 1992
- *Guide to Threat and Risk Assessment for Information Technology* (SIP 5), RCMP, November 1994
- *Identification Cards/Access Badges* (SSB/SG-27) June 1992
- *Security Equipment Guide* (SSB/SG-20), October 1992 (Distribution restricted to federal government departments and not available electronically.)
- *Standard for the Transport and Transmittal of Sensitive Information and Assets* (SSR/SG-30), June 1994

TREASURY BOARD SECRETARIAT PUBLICATIONS

- *Federal Identity Program Manual*, March 1990
- "Fire Protection Standard for Electronic Data Processing Equipment", *Treasury Board Manual, Occupational Safety and Health*, Chapter 3-3.
- *Security volume, Treasury Board Manual* (Cat. No. BT52-6/3), commonly known as the "Government Security Policy" (GSP).

COMMUNICATIONS SECURITY ESTABLISHMENT PUBLICATIONS

- *COMSEC Installation Planning* (TEMPEST Guidance and Criteria) (CID/09/7A), 1983, (English only)(Confidential)
- *COMSEC Planning - TEMPEST Guidance* (CID/09/7)
- *Controlled Cryptographic Items (CCI) Manual* (CID/01/08), March 1992 (Unclassified)
- *Criteria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-In Radio Frequency Shielded Enclosures* (CID/09/12A)(Unclassified)
- *CSE-Approved Degaussers for Erasure of Magnetic Media* (CTIB 7/96)
- *Guidelines for Clearing and Declassifying Automatic Data Processing Storage Devices* (CTIB 19/87)
- *INFOSEC Materiel Control Manual* (CID/01/10), September 1991, Interim Release (Protected A)
- *Specifications for the Design, Fabrication, Supply, Installation and Acceptance Testing of Radio Frequency Shielded Enclosures* (CID/09/12)
- *The Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0e (CID 09/19), January 1993 (Unclassified)

OTHER GOVERNMENT DEPARTMENTS PUBLICATIONS

- *Guide to the Audit of Security* (OCG Guide 406)
- *Industrial Security Manual*, (Supply and Services Canada, 1992)
- *National Building Code of Canada* (National Research Council)
- *Record Storage*, FC 311(M) (Fire Commissioner of Canada)

PRIVATE AGENCY PUBLICATIONS

- Underwriters' Laboratories of Canada Standards