Information Technology Security Requirements:

Handling Sensitive Information at Contractor Premises

Date Issued: 11 June 2012

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to specify Information Technology Security (ITS) requirements for Immigration and Refugee Board (IRB) sensitive information handled onsite at contractor premises. ITS requirements define a minimum set of security safeguards to be implemented for proper protection of the information.

This document is intended to assist a contractor in achieving a minimum level of security based on principles and requirements of the Policy on Government Security (PGS) and associated Government of Canada (GoC) directives, guidelines and standards.

The document is to be used as the basis for preparing a Request for Proposal (RFP) response by contractors during a procurement process. Once a contract has been awarded, an independent ITS Review by the IRB IT Security Coordinator (ITSC) will be conducted to grant approval to capture, process and store IRB sensitive information onsite at contractor premises.

1.2 Focus

The focus of the security requirements is placed on ensuring the **Confidentiality** of information captured, processed and stored at contractor premises. Confidentiality, as defined by the PGS, is the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*.

1.3 Scope

Sensitive information handled onsite site at contractor premises must be treated in the same manner as within an IRB facility. These IT security requirements are meant to protect the confidentiality of IRB information assets rated up to and including the level of **Protected B**. As defined in the Identification of Assets guideline published by Treasury Board Secretariat (TBS), if Protected B information is compromised this could reasonably be expected to cause a serious injury to private or non-national interests. If applicable, prime contractors are responsibility for ensuring all sub-contractors comply with all of the requirements defined herein.

1.4 Methodology

The ITS requirements are based on federal government of Canada policies, directives, guidelines and standards. The requirements are principally derived from the TBS Management of Information Technology Security (MITS) operational security standard and the Guide to Managing Security Risks from Using Information Systems (ITSG-33) published by the Communications Security Establishment Canada (CSEC).

2. Contractor Organization and Security Screening

Security is based upon multiple layers of protection; that is, in order for the requirements of the ITS to effectively safeguard information, they must be preceded and supported by other aspects of security and the associated policies. Security safeguards identified in this section must exist **prior** to implementation of the ITS safeguards defined in Section 3.

2.1 Security Organization

The contractor must appoint a Company Security Officer (CSO) and an Alternate Company Security Officer (ACSO).

The CSO is responsible for the development, implementation, maintenance, coordination, and audit of company security policies, standards and procedures, to ensure:

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

When requested by the IRB, the name and contact coordinates of the CSO must be provided to the IRB DSO who will notify the ITSC.

All CSO/ACSOs must attend a security training and awareness session coordinated and delivered by the IRB Departmental Security Officer (DSO) and ITSC.

2.2 PWGSC Validation of Physical Security

The implementation of ITS safeguards listed in this document are based on the mandatory requirement that the contractor's physical premises have been inspected, certified and accredited to process and store sensitive information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC). The contractor must obtain and hold a valid Designated Organization Screening (DOS) issued by CISD.

The IRB Departmental Security Officer (DSO) will validate the DOS with CISD and notify the IRB ITSC before an IT security review is conducted.

2.3 Personnel Security

All contractor personnel who are to have access to IRB sensitive information must hold a valid **Reliability Status** Personnel Security Clearance). Persons who have been granted a Personnel Security Clearance may only have access to Protected information, assets or sites on a "need-to-know" basis.

The IRB DSO, or his/her delegate, will validate the security clearance of all contractor personnel and notify the IRB ITSC.

All contractor personnel handling IRB sensitive information must first attend a security training and awareness session coordinated and delivered by the CSO before being granted access to the information.

2.4 Electronic Data Processing (EDP) Document and Data Production

Once a contractor has been awarded a contract through PWGSC or IRB to electronically process Protected information on their IT system, the contractor must request CISD conduct an EDP Document and Data Product Review.

A report containing recommendations and suggestions will be prepared by CISD and forwarded to the organization's CSO. Implementation of the recommendations is mandatory, and any suggestions, while not mandatory, should be considered for follow-on remediation action.

The IRB DSO, or his/her delegate, will validate the EDP Document and Data Product Review clearance and notify the IRB ITSC.

2.5 Information Security

All hard copy documents and documents stored on digital media (e.g. CDs/DVDs) must be handled and transported in accordance with GoC directives and guidelines. All hard copy documents and other media must be marked with the appropriate security classification as designated by the IRB. Any covering letter, transmittal form or circulation slip must be marked to indicate the highest level of classification of the attachments.

Transportation of information associated with this contract into or out of the contractor’s physical premises must adhere to RCMP G1-009 Transport and Transmittal of Protected and Classified Information.

2.6 Security Compliance Monitoring

On a frequency to be determined by the DSO and/or ITSC, the IRB retains the right to conduct regular or periodic inspections of the contractor’s facility to ensure compliance with GoC policies for handling, storage and processing of IRB sensitive information.

3. Information Technology Security Controls

A Security Control Catalogue is a singular source for a set of baseline security controls (i.e. safeguards or countermeasures) that can be deployed to protect the confidentiality, integrity, and availability of information systems. The catalog was developed by the CSEC using content from the National Institute of Science and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems. Security control definitions have been modified and augmented to adapt the catalogue to a GoC context.

The process used to derive the security requirements for an information system is comprised of security control categorization and tailoring. The security control families and classes have been tailored in the section which follows to focus on protecting the confidentiality of information. The new security control baseline resulting from the tailoring process is referred to as a “tailored security controls baseline”. The tailored security control baseline for contractors holding IRB sensitive information up to and including the level of Protected B can be found in Appendix B.

There are two general classes of security controls – operational and technical - selected from the Security Control Catalogue that form the basis for these security requirements to protect the confidentiality of information assets. The following definitions of the two different classes of security controls are:

a. **Operational Security Controls** - The security controls (i.e. safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems); and

b. **Technical Security Controls** - The security controls (i.e. safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Each class of security controls (i.e. operational and technical) is further divided into families of security controls. The operational security control class consists of the following security control families selected are:

a. **Awareness and Training (AT)** - Security controls that deal with the education of users associated with the information system on security awareness;

b. **Incident Response (IR)** - Security controls that support the detection, response and reporting of security incidents within the information system;

c. **Media Protection (MP)** - Security controls that support the protection of information system media (i.e. disks, tapes, etc) throughout their life cycle; and

d. **Personnel Security (PS**) - Security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate clearances;

The technical security control class consists of the following security control families selected are:

a. **Identification and Authentication (IA)** - Security controls that support the unique identification of users and the authentication of these users when attempting to access the information system;

b. **Access Control (AC)** - Security controls that support the ability to permit or deny user access to resources within an information system;

c. **Audit and Accountability (AU)** - Security controls that support the ability to collect, analyze and store audit records associated with user operations performed within the information system; and

d. **System and Communications Protection (SC)** - Security controls that support the protection of the information system itself as well as communications with and within the information system.

Appendix A: Acronyms and Abbreviations

Acronym / Abbreviation	Full Name
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
ACSO	Acting Corporate Security Officer
CISD	Canadian Industrial Security Directorate
CSEC	Communications Security Establishment Canada
CSO	Corporate Security Officer
DOS	Designated Organization Screening
DSO	Departmental Security Officer
EDP	Electronic Data Processing
GoC	Government of Canada
IA	Identification and Authentication
IR	Incident Response
IRB	Immigration and Refugee Board of Canada
IT	Information Technology
ITS	Information Technology Security
ITSC	Information Technology Security Coordinator
ITSG	Information Technology Security Guidance
MITS	Management of Information Technology Security
MP	Media Protection
PGS	Policy on Government Security
PS	Personnel Security
PWGSC	Public Works Government Services Canada
RCMP	Royal Canadian Mounted Police
RFP	Request For Proposal
SC	System and Communications Protection
TBS	Treasury Board Secretariat

Appendix B: Tailored Security Controls Baseline

Note: While selecting security controls can be subjective, considerable effort was made to include only those security controls that mitigate real threats to disclosure and loss of confidentiality of particularly sensitive Protected B information, and that can be implemented using readily available commercial-off-the-shelf (COTS) products. Security controls that specify a specialized or advanced capability not required for an information system were excluded from this tailored security profile baseline. Every effort was made to achieve an appropriate balance between usability and security and security and cost-effectiveness.

Control ID	Name	Definition	Supplemental
Operational Security Controls			
Awareness and Training (AT)			
AT-2	Security Training	The organization provides security-related training to all users before authorizing access to the system or performing assigned job duties.	The organization shall determine the appropriate content of security training based on material provided by the IRB to the CSO.
Incident Response (IR)			
IR-1	Incident Response Procedure	(A) The organization develops, disseminates, and reviews/updates a documented procedure to facilitate the implementation of incident response to security incidents. The incident response procedure: (a) Provides the organization with a high level approach for implementing its incident response capability; (b)Describes the structure and organization of the incident response capability; (c)Defines reportable incidents; (d)Is reviewed and approved by designated officials within the organization. (B) The organization distributes copies of the incident response plan to all users of an information system. (C)The organization reviews and updates as necessary the	It is important that organizations have a formal, focused, and coordinated approach to responding to incidents.

Control ID	Name	Definition	Supplemental
		incident response procedure at least every three (3) years.	
IR-2	Incident Response Training	The organization trains personnel in their incident response roles and responsibilities with respect to the information system as part of security training (refer to control AT-2).	
IR-4	Incident Handling	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	All security incidents must be brought to the attention of the CSO upon occurrence or detection by any organizational employee/contractor.
IR-5	Incident Monitoring	The organization tracks and documents information system security incidents.	Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
IR-6	Incident Reporting	(A)The organization requires personnel to report suspected security incidents to the CSO. (B)The organization reports all security incident information to the CSO within twenty four (24) hours. (C) The CSO investigates each security incident. All security incident reports must be submitted to the IRB DSO within seventy two (72) hours from the time an incident is first reported to the CSO.	The intent of this control is to address both specific incident reporting requirements within a contractor organization and the formal incident reporting requirements for the IRB. The types of security incidents reported, the content and timeliness of the reports and the list of designated reporting authorities are to be consistent with applicable GC legislation and TBS policies, directives and standards.

Control ID	Name	Definition	Supplemental
MP-1	Media Protection	The organization restricts access to digital media storing sensitive information to authorized users only. Digital media includes external/removable hard drives, flash/thumb drives, compact disks, digital video disks, etc.).	Mobile computing and communications devices with information storage capability (e.g., personal digital assistants, cellular telephones, smart phones, and digital cameras) shall not be used with an information system holding IRB sensitive information rated Protected B.
MP-2	Media Access	The information system uses cryptographic encryption mechanisms to protect and restrict access to information rated as Protected B stored on portable digital media (e.g., USB sticks, flash/thumb drives, etc.).	
MP-3	Media Marking	The organization marks, in accordance with government standards, all removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Refer to the TBS Security Organization and Administration Standard for guidance.	
MP-4	Media Storage	(A)The organization physically controls and securely stores all digital media within organization-defined controlled Operations Zones in accordance with the RCMP G1-001 Security Equipment Guide. (B)The organization physically protects and securely stores Protected B information system media awaiting destruction (either on- or off-site) using government approved equipment, techniques, and procedures.	

Control ID	Name	Definition	Supplemental
MP-5	Media Transport	(A)The organization protects and controls digital media during transport outside of controlled areas using in accordance with the TBS Operational Security Standard on Physical Security and the RCMP G1-009 Transport and Transmittal of Protected and Classified Information. (B)The organization maintains accountability for information system media during transport outside of controlled areas. (C)The organization restricts the activities associated with transport of such media to authorized personnel. (D) The organization documents activities associated with the transport of information system media. (E) The organization employs an identified custodian throughout the transport of information system media.	
MP-6	Media Sanitization	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of sensitive information to unauthorized individuals when such media is reused or released for disposal.

Control ID	Name	Definition	Supplemental
PS-6	Access Agreements	The organization ensures that individuals requiring access to information systems and IRB sensitive information sign appropriate access agreements prior to being granted access.	Access agreements include, for example, nondisclosure agreements, acceptable use agreements, and rules of behaviour. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system and information to which access is authorized.
Technical Security Controls			
Identification and Authentication (IA)			
IA-2	Identification and Authentication (Organizational Users)	(A) The information system uniquely identifies and authenticates organizational users. Organizational users include organizational employees or individuals the organization deemed to have equivalent status of employees (e.g., contractors). (B) Users must be uniquely identified and authenticated for all accesses to an information system.	Authentication of user identity can be accomplished through the use of passwords, certificates, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.
IA-4	Identifier Management	(A)The organization manages information system identifiers for users (i.e. user IDs) by receiving authorization from a designated organizational official to assign a user identifier. (B)The organization selects an identifier that uniquely identifies an individual. (C)The organization disables the user identifier after one hundred and eighty (180) days of inactivity.	

Control ID	Name	Definition	Supplemental
IA-5	Authenticator Management	(A)The organization manages information system authenticators for users by verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator. (B)The organization manages information system authenticators for users by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. (C)The organization changes default content of authenticators upon information system installation (i.e. do not use default authenticators). (D)The organization establishes minimum and maximum lifetime restrictions and reuse conditions for authenticators. (E)The organization changes/refreshes authenticators at least annually. (F)The organization protects authenticator content from unauthorized disclosure and modification.	User authenticators include, for example, passwords, tokens, biometrics, certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, must be changed upon installation.

Control ID	Name	Definition	Supplemental
IA-5	Authenticator Management	For password-based authentication, the information system must: (a) Comply with the IRB Password Policy; (b) Enforce minimum password complexity in accordance with Annex A – Password Construction Standards of the IRB Password policy; and (c)Encrypt all passwords in storage and in transmission.	
IA-6	Authenticator Feedback	(A)The information system obscures feedback of authentication information during an authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.
Access Control (AC)			

Control ID	Name	Definition	Supplemental
AC-2	Account Management	(A)The organization manages information system accounts, including identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary). (B)The organization identifies authorized users of the information system and specifies their access control privileges. (C)The organization manages an appropriate approval process for requests to establish user accounts. (D)The organization creates, activates, modifies, disables, and deletes user accounts. (E)The organization notifies responsible managers when users are terminated, transferred, or need-to-access the system changes. (F)The organization deactivates accounts of terminated or transferred users. (G)The organization manages reviews all accounts for continued need-to-access at least annually.	
AC-7	Unsuccessful Login Attempts	(A) The information system enforces a limit of five (5) consecutive invalid login attempts by a user. (B) The information system automatically locks the account until the lock is released by an administrator.	

Control ID	Name	Definition	Supplemental
AC-8	System Use Notification	(A)The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on the Use of Electronic Networks. (B)The information system retains the notification message or banner on the screen until users take explicit actions (e.g. clicks on an <accept> button) to log on to the information system.	
AC-17	Remote Access	**Remote access to an information system is not permitted to an information system holding IRB sensitive information**.	Remote access is any access to the information system by a user communicating through an external network (e.g. Internet, wireless network, cellular network, etc.). Access to an organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user where such access is obtained through a network connection. Network access will be permitted only on local area networks that are logically and physically isolated from all other internal and external networks used by the organization.

Control ID	Name	Definition	Supplemental
AC-18	Wireless Access	**Wireless access to an information system is not permitted to an information system holding IRB sensitive information**.	Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11, and Bluetooth. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.
AC-19	Access Control for Mobile Devices	**Access to an information system using mobile devices is not permitted to an information system holding IRB sensitive information**.	Mobile devices include portable computing and communications devices with information storage capability (e.g., personal digital assistants, cellular telephones, and smart phone communicating over a cellular network or the Internet.
Audit and Accountability (AU)			
AU-2	Auditable Events	The information system audits the following user/process events at a minimum: (a) Successful and unsuccessful user logon attempts; (b) Starting and ending time for user access to the system; and (c) All program initiations.	
AU-3	Content of Audit Records	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user associated with the event.	

Control ID	Name	Definition	Supplemental
AU-6	Audit Review, Analysis and Reporting	The organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to the CSO.	
AU-8	Timestamps	The information system uses trusted system clocks to generate time stamps (date and time) for audit records.	Clocks may be synchronized automatically with a trusted time source using a protocol such as the Network Time Protocol (NTP), or the organization may implement a manual procedure to ensure correct date and time on all computers hosting an information system.
System and Communications Protection			
SC-7	Boundary Protection	(A) The information system shall not connect to external networks (e.g., other corporate local networks, wide area networks and the Internet). (B)The organization limits the number of access points to the information system to allow for monitoring of network traffic. (C) The organization protects and monitors against unauthorized physical connections across boundary protections.	Boundary protection devices include, for example, proxies, gateways, routers, firewalls, and guards.
SC-9	Transmission Confidentiality and Integrity	The information system protects the confidentiality and integrity of information transmitted across internal networks.	

Control ID	Name	Definition	Supplemental
SC-13	Use of Cryptography	Where required, the information system implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.	The baseline control requires the use of CSEC-approved cryptographic algorithms, which include, in addition to algorithms, approved key lengths, cryptoperiods, modes of operations, padding schemes, and number bit generation, as described in ITSA-11D CSEC Approved Cryptographic Algorithms for the Protection of Protected Information.
SC-28	Protection of Information at Rest	The information system protects the confidentiality and integrity of information at rest.	This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user, system and database information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive). Configurations and/or rule sets for routers, switches, firewalls, and authenticator content are examples of system information requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.