



Immigration, Refugees and Citizenship Canada

Immigration, Réfugiés et Citoyenneté Canada

Privacy and Security Requirements for Funding Recipients

Immigration Contribution Agreement Reporting Environment



Immigration, Refugees and Citizenship Canada



CONTENTS

- Introduction 1
- Part I: Privacy Requirements 2
 - Background 2
 - Personal Client Information 2
 - Definition of 'Protected' Information 2
 - Core Principles for the Handling of Client Information 2
- Part II: iCARE Minimum Security Requirements checklist 6
 - Background 6
 - Submitting the iCARE Minimum Security Requirements checklist 7
- Part III: Technological Security Requirements 8
 - Background 8
 - Minimum Technological Security Requirements 8
 - Firewall 9
 - Anti-Virus/Anti-Malware 9
 - Networks and Networked Computers 9
 - Security Patches 10
 - Security Settings 10
 - Web-Browser 11
 - Password Protection and lock 11
 - Additional Security Measures 11
 - USB keys and other portable storage devices 11
 - Cloud storage services and servers 12
 - WI-FI 13
 - Email 13
 - Intrusion Detection 14
 - Content Inspection 14
 - How to respond when a computer or IT system is infected with a virus or malware 14
 - TIPS to Prevent further Infections: 15
- Part IV: Physical Requirements 16
 - Background 16

Minimum Physical Requirements	16
Additional Physical Requirements:	17
Password protection.....	17
Printing and Document Handling	17
Part V: User Requirements	17
Background	17
User Reliability Assessment	17
1. Obtaining Consent.....	18
2. The Criminal Record Check.....	18
3. Verification of Information.....	20
4. The Reliability Assessment Decision.....	20
5. A Positive Reliability Assessment.....	21
6. The Security Briefing	21
7. Completing the iCARE User Account Request Form	21
8. Cancelling an iCARE Account	22
Reliability Assessment Records	22
Retention	22
Disposal	22
Access	22
User Requirements Checklist	22
Part VI: Organizational Security Policies and Training	23
Background	23
Training Requirements.....	23
Procedures and Policies.....	23
Part VII: Privacy Breaches and Violations	24
Background	24
Privacy Breaches – Guidance for Funding Recipients	25
Potential Causes of Privacy Breaches	25
How to Respond to a Privacy Breach	25
Appendix A - iCARE Minimum Security Requirements.....	28
Appendix B – Wireless Recommendations	30
Appendix C: Example of a Protocol for Handling Sensitive Material	31



Appendix D – iCARE User Reliability Assessment Form 33
Appendix E: iCARE User Reliability Assessment Table 35



Introduction

Immigration, Refugees and Citizenship Canada (IRCC) has a legal requirement under the *Privacy Act*, which it extends to Funding Recipients through the Contribution Agreement, to ensure that personal client information is safeguarded according to security and privacy standards. The security and privacy standards outlined in this document are based on advice received from IRCC's internal privacy and security experts. It is important that both Funding Recipients and IRCC staff understand the key policy and legislative principles which govern the handling of personal client information on which the security and privacy standards are based. Adopting these standards will ensure that IRCC and Funding Recipients are taking a consistent approach to the protection of personal client information collected. IRCC is also making a series of recommendations that it encourages Funding Recipients to implement, along with any additional policies and procedures they deem necessary to protect their clients' personal information.

The information provided in this document is particularly relevant for the use of IRCC's Immigration Contribution Agreement Reporting Environment (iCARE). This system allows for the collection of client and service information on the Settlement and Resettlement Programs delivered to eligible clients.

In addition to this manual, Funding Recipients should familiarize themselves with the privacy and security obligations found in section 7.0 of the contribution agreement (CA). Personal client information collected or maintained by the Funding Recipient within Canada is subject to the provisions of the applicable federal, provincial/territorial privacy and access to information legislation or the *Personal Information Protection and Electronic Documents Act*. Funding Recipients providing services outside of Canada must comply with national or domestic laws of the countries where their services are being provided. However, they must also ensure that they meet the requirements found in the contribution agreement and those found in this manual.

Data is collected in iCARE according to the following modules for both domestic and pre-arrival services:

- Pre & Post Arrival Needs Assessment and Referrals
- Pre & Post Arrival Employment Related Services
- Post Arrival only Language Assessment and Training Services
- Pre & Post Arrival Information and Orientation Services
- Pre & Post Arrival Community Connections Services
- Post Arrival Only Resettlement Assistance Program (RAP).
- Pre & Post Arrival Narrative Report/Annual Project Performance Report (APPR).

Part I: Privacy Requirements

Background

IRCC is required to protect personal client information under federal privacy legislation. This requirement is extended to Funding Recipients through the Contribution Agreement, as they are collecting this information on behalf of IRCC. Further details of Funding Recipient's responsibilities for the secure protection of personal client information can be found under section 7 of the Contribution Agreement.

In order to meet its obligations under federal privacy legislation, IRCC must introduce specific privacy and security requirements for the purpose of collecting personal client information. These requirements are outlined in this document and include technological, physical, personnel and organizational security measures. It should be noted that the adoption of these types of measures is good practice for any environment where personal client information is collected and stored.

Personal Client Information

Information collected in iCARE is considered personal in nature. Security and Privacy Assessments have designated this information as 'Protected B' because unauthorized disclosure could reasonably be expected to cause serious injury.

Definition of 'Protected' Information

- **Protected A** information includes unique identifiers such as national or ethnic origin, religion, age, marital status, date of birth, any identifying number or symbol (e.g., GCMS or FOSS Client Identifiers), program-related client records, language educational progress records, language training assessments and/or employment related documents.
- If this basic information can be used to uniquely identify an individual, it is **Protected B** (e.g. if this information is further combined with personal client information related to settlement and resettlement program services provided to the individual, it would be designated as Protected B information).

Core Principles for the Handling of Client Information

The Funding Recipient is obligated under the contribution agreement (CA) to observe the following practices in the delivery and administration of settlement and

resettlement services on behalf of IRCC, where such activities involve the use of personal client information as described above.

1. Be open about why the information is being collected

Funding Recipients must advise clients of the purposes for which their information is to be collected, used, disclosed and retained prior to the delivery of IRCC-funded services.

IRCC collects personal client information to better understand newcomers' needs. With this information, we can ensure that Funding Recipients are performing well, decide how IRCC can improve the services funded, and report to the public about how these programs are working. Funding Recipients can also use this information to help plan and manage these programs and the services provided.

Funding Recipients must make available to all IRCC clients receiving services under an IRCC-funded agreement, an electronic or paper version of the "Gathering Information" pamphlet (which can be found in the iCARE Resources tab), or assist in the reading and review of the pamphlet's contents, which explains the purposes for which personal client information is to be collected, used, disclosed and retained. Funding Recipients must inform clients of the reason for the collection of the information when clients receive their first service. The Funding Recipient should then remind the client of this purpose periodically, at reasonable intervals. Funding Recipients should keep a record of this in their client file.

Clients may also be referred to IRCC's *Info Source* publication, available on-line at www.cic.gc.ca/english/departement/atip/infosource/pibs.asp, which provides more details on the collection of personal client information.

2. Only collect information that is needed

Funding Recipients must limit collection of personal client information to that which is necessary for delivering IRCC-funded programming.

Funding Recipients will limit collection of personal client information to only that which is necessary to carry out programming, and must be proportional to the benefit to be derived from the expected outcomes of the project. The collection of additional information for the purpose of settlement and/or resettlement programming, however helpful, is not authorized. If the Funding Recipient is unsure about whether additional information is needed for IRCC-funded program delivery and reporting, please contact IRCC.

Should the Funding Recipient need to collect personal client information elements beyond those required by IRCC, they must either meet applicable privacy legislation or obtain the consent of the client to collect this additional information. The



additional information must also be physically and logically segregated from information and records that the Funding Recipient has collected for IRCC purposes. This segregation must be set up in such a way as to ensure that IRCC specific information can be removed from systems or files. For example, an IRCC client ID should not be used by the Funding Recipient to number client files as it would be difficult to remove the IRCC client ID for a client who continues to receive services from the organization but is no longer accessing IRCC funded services.

3. Ensure the information collected is accurate and complete and is made available to the client.

Funding Recipients must take reasonable steps to ensure that the client information collected and inputted in iCARE is as accurate, up-to-date, and as complete as possible.

Funding Recipients can generally presume that information collected directly from a client is accurate and complete. Where information about a client appears to be inconsistent with the information on record, Funding Recipients must take additional steps to ensure that their records are accurate. The discovery of adverse or conflicting information should be brought to the client's attention for clarification and correction. If the issue resides with IRCC, for example the name of the client is spelled incorrectly in iCARE, the client must contact IRCC.

In addition, clients must be given access to their own information, including service records, upon request. The client may verify and challenge the accuracy and completeness of the information, and request to have it amended as appropriate. The Funding Recipient is responsible for correcting their own records where required. If the information has already been inputted into iCARE and it is discovered that this information is incorrect, the Funding Recipient should contact the iCARE helpdesk for guidance.

4. Only use client information as authorized

Funding Recipients will only use personal client information under their control for the purposes for which it was first collected.

Information collected from and about clients is to be used strictly for settlement and resettlement programming purposes. The use of personal client information, alone or in aggregate, for secondary purposes must be authorized by the client by obtaining their written consent.

5. Don't share or disclose personal client information

Personal client information collected for IRCC purposes and under a Funding Recipient's control shall not be disclosed to others, except in accordance with applicable law.

Personal client information collected for IRCC purposes is to be treated as confidential. It cannot be disclosed to anyone other than the client to whom the information belongs, except where authorized by applicable law.

6. Securely destroy personal client information that is no longer needed

Funding Recipients will only retain personal client information for so long as it is needed for programming and reporting purposes.

Funding Recipients should only retain personal client information that has been entered into the IRCC- approved data collection system (e.g., iCARE) for as long as the client continues to receive services, after which it should immediately be disposed of in a manner that is appropriate to its level of classification or designation.

Where such information will not be entered into the IRCC data collection system (e.g., pilot project participant information, workshop participant surveys, etc.), the recipient should retain it for no more than two years after the project file close-out has been completed for the agreement under which the client last received services, after which the protected information must be disposed of. This will allow client records to be retained beyond the life of a single agreement where the client continues to receive services under succeeding agreements.

If the Funding Recipient is required to retain the personal client information beyond either of the above retention periods for purposes outside of IRCC-funded activities, for example services provided to clients through other funders, all IRCC-specific client identification information (e.g., FOSS or GCMS number), must be removed from Funding Recipient paper and electronic records. Note that this does not include iCARE records as IRCC has specific Retention and Disposition Schedules for data collected in the system.

7. Keep personal client information safe and secure

Funding Recipients must protect personal client information in a manner appropriate to the sensitivity of the information collected.

Funding Recipients are responsible for putting security measures in place to protect the information they collect from and about clients. These security provisions must meet the minimum security requirements established by IRCC, as set out in this

manual and in the CA. Funding Recipients must attest that they are meeting these minimum requirements through the completion and submission of the iCARE Minimum Security Requirements (MSR) checklist.

8. Be accountable for the manner in which personal client information is handled

Funding Recipients are responsible for personal client information under their control and should designate an individual accountable for the organization's compliance with the above principles.

Funding Recipients are subject to the monitoring of their personal client information handling practices. IRCC may undertake or request an audit or other compliance review of these practices. Holding an individual accountable for the organization's compliance with the above principles helps to ensure that the organization remains accountable to IRCC and clients alike.

Part II: iCARE Minimum Security Requirements checklist

Background

As per the conditions outlined in the Contribution Agreement, Funding Recipients are required to comply with the security standards outlined in the iCARE Minimum Security Requirements (MSR) Checklist. The MSR is a comprehensive checklist that addresses the minimum security conditions each Funding Recipient must have in place while dealing with personal client information. As such, Funding Recipients are required to complete the MSR checklist to identify whether they are meeting IRCC's security standards, or if improvements need to be made. Failure to meet the minimum security requirements may result in access to the iCARE system being denied.

The MSR checklist identifies four key areas of security compliance for Funding Recipients:

- Technological Security Requirements
- Physical Requirements
- User Requirements
- Organizational Security Policies and Training

These security areas will be explained in detail in the following sections. The MSR checklist can be found in Appendix A.

Funding Recipients must meet the MSR checklist requirements to access iCARE. However, an organization can also use the MSR checklist for the following:

- to identify the organization’s capacity to meet IRCC security requirements and bring this information into the discussions when negotiating the terms of the contribution agreement;
 - if an organization identifies weaknesses or a gap in its security posture, funds may be available within the contribution agreement to cover the cost of meeting IRCC security requirements (e.g., upgrades to anti-virus software);
- to track an organization’s progress towards compliance with IRCC’s security requirements;
- after signing the contribution agreement, to determine if an organization has all necessary elements in place to ensure compliance with IRCC’s security requirements—or, will have all necessary elements in place very shortly.

Submitting the iCARE Minimum Security Requirements checklist

All Funding Recipients reporting in iCARE are required to submit a completed MSR checklist. If the funding recipient has multiple contribution agreements, thus having multiple iCARE accounts, they must submit a MSR checklist for each CA and its associated account. If there are multiple CAs which are for the same physical location, the same PDF document can be uploaded to each account. However, a new MSR should be completed and uploaded for an account that represents a CA for a different location.

If an organization has multiple locations for one CA the Funding Recipient must only complete one MSR checklist. However, each location must meet the security requirement in order to check “yes” on the checklist. If a location does not meet the security requirement, then the Funding Recipient must check “no” and explain in the client response section which location does not meet the security requirement and what steps will be taken to meet the requirement in that particular location.

The MSR checklist is to be completed by the Executive Director (ED) or a designate, as identified in iCARE.



Note: The signatory to the CA, or an individual with signing authority, is considered the Executive Director (ED) of the organization for iCARE purposes. As the signing authority, this individual must always have an active iCARE account; however, the ED is able to designate other iCARE users to have ED designate authority.

The MSR checklist must be submitted through iCARE after the ED has initialized the iCARE ED account for that CA. If a MSR checklist is not uploaded, the account may be locked. This would mean that no data could be entered by any user who is associated with that CA. Should a Funding Recipient have concerns about the MSR checklist they should contact IRCC.

How to download the MSR checklist:

- Click the "Security" tab on the iCARE homepage;
- Click the "Minimum Requirements Checklist" link under "Checklist Forms" to download a copy;
- Complete and save a copy of the checklist.

How to Submit a MSR checklist:

- Click the iCARE "Security" tab;
- Select the File Type: "Minimum Requirements Checklist";
- Click the Browse button and upload the **completed** copy of the MSR checklist.

Funding Recipients that do not meet the security requirements outlined in the MSR checklist at the time of obtaining an iCARE account should still submit the checklist in iCARE. Organizations are then required to take necessary actions to improve security conditions, as well as provide IRCC with updates, to address all outstanding security requirements. The ED, or designate, must submit an updated MSR when steps have been taken to meet all requirements.

Part III: Technological Security Requirements

Background

The technological security requirements outlined in the MSR checklist are intended to ensure the confidentiality and integrity of information stored, processed or transmitted electronically. As a minimum, these security measures include password protected computers, encryption of data, and up-to-date firewall and anti-virus software. Compliance with these security standards is required for access to iCARE and is good practice for any environment handling personal client information

Minimum Technological Security Requirements

The following minimum technological security standards, as outlined in the MSR checklist, must be met:

Firewall

Firewalls are used to limit and screen traffic going to and coming from a network or computer by receiving and transmitting information only over specific ports, making it much more difficult for outside threats to take control of the system by accessing open ports.

All computers handling personal client information must have up to date firewall software

This must be used at both the network and individual workstation level.

When choosing a firewall it is up to the Funding Recipient to assess operational needs and select a product which meets those needs.

Anti-Virus/Anti-Malware

All computers handling personal client information must have anti-virus/anti-malware software which must be kept up to date. This must be used at both the network and individual workstation level.

When choosing an anti-virus/anti-malware it is up to the Funding Recipient to assess operational needs and select a product which meets those needs.



Note: Virus/malware protection software requires regular updating (which can be weekly) in order to effectively detect new viruses/malware. The instructions provided with the software package will explain how to do this.

Networks and Networked Computers

In the case of computers connected through a network the network itself should be equipped with protection specifically designed for it. For this reason, IRCC is **recommending** the following for networks and networked computers:

- Funding Recipients using a network (or using someone else's network, such as a school board, etc.) ensure its protection through the use of (as a minimum) network-specific firewall and anti-virus/anti-malware technology; and
- Funding Recipients install anti-virus/anti-malware software on individual workstations connected to the network.

Funding Recipients running networks without network-specific firewall and anti-virus/anti-malware protection software are required to access iCARE on stand-alone computers that meet the firewall and anti-virus/anti-malware requirements outlined above.

Security Patches

A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called “bugfixes” or “bug fixes”, and improving the usability or performance. These patches are released by the software developers.

Funding Recipients are expected to test and deploy promptly on networks and computers, patches which are released for the software they are using.

All Windows operating systems can be kept up to date with regular Microsoft updates. All other software installed must also be kept up to date by applying any applicable patches and updates issued by the applicable vendor(s).

Funding Recipients should have procedures in place which establish patch roll out process and schedule.

Security Settings

Funding Recipients are expected to keep up to date and monitor their computer and network security settings. These should be maintained and reviewed periodically to ensure that they meet requirements for handling sensitive information.

Workstations and servers are to be hardened (secured) to ensure that only the features and functionality required are enabled, without detriment to the operating system.

Hardening activities for a computer system can include:

- Keeping security patches updated
- Monitoring security bulletins that are applicable to a system’s operating system and applications
- Installing a firewall
- Closing certain ports such as server ports
- Not allowing file sharing among programs
- Installing virus and spyware protection, including an anti-adware tool so that malicious software cannot gain access to the computer on which it is installed
- Keeping a backup, such as a hard drive, of the computer system
- Disabling cookies
- Creating strong passwords
- Never opening emails or attachments from unknown senders
- Removing unnecessary programs and user accounts from the computer
- Using encryption where possible

- Hardening security policies, such as local policies relating to how often a password should be changed and how long and in what format a password must be in.

Web-Browser

Funding Recipients must access iCARE and input personal client information using the latest version of web browsers available. iCARE uses the latest client/server encryption to protect data in transit: Transport Layer Security (TLS). A Web Browser that uses the latest version of TLS must be used (e.g. Internet Explorer version 11, Firefox X or higher, or Chrome. TLS 1.0, 1.1 or 1.2 must be enabled when using these Web Browsers).

Note that at this time iCARE is only supported by Internet Explorer, however, other Web Browsers may work.

Password Protection and lock

For added security, and to safeguard against unauthorized access, computers used for iCARE must have unique account credentials to access those computers (username and password). We recommend that the password be changed every 3 months or 90 days.

In addition, a screen-saver with password protection with an activation period of no more than 15 minutes of non-usage must be implemented.

Additional Security Measures

Beyond the MSR checklist, to meet Section 7 of the CA, the following technological security measure should be implemented:

USB keys and other portable storage devices

The improper use and handling of portable data storage devices or the improper storage of personal client information on these devices can pose significant risks to the security of client information and may violate policies for security, privacy protection and information management as per the contribution agreement.

Portable data storage devices are devices that are easily movable and contain storage or memory into which users can transfer and store information.

Examples of portable data storage devices include:

- USB devices (e.g. memory sticks, external hard drives);
- eSATA (External Serial Advanced Technology Attachment) devices;
- Tablets, laptops, smart devices (e.g. BlackBerry), and cameras; and

- Portable media – tapes, optical discs (e.g. CDs and DVDs).

Portable data storage devices must be properly secured at all times. If they contain personal client information they should be kept locked up. They must be labeled to indicate that they contain Protected B information using an indirect coding system that is not immediately recognizable to the general public (examples are barcodes, colour codes or numbering schemes).

To transfer personal client information, portable devices must be encrypted with Entrust desktop software. If Entrust desktop software is not available encrypted USB drives can be used. The minimum level of encryption required is: FIPS 140-2 Level 3 certified.

Portable data storage devices are intended for the temporary storage of information only and must not be used as permanent document repositories to store personal client information.

When the information is no longer needed the portable data storage device must be “cleared”. Clearing is the process of erasing stored information from portable data storage devices in a manner that allows it to be re-used within an equivalent security environment.

Clearing must be adequate to prevent information recovery using tools normally available on the Information System. Simply deleting or erasing the files or reformatting may not clear the portable data storage device, because commands such as undelete or un-format may permit the recovery of the information. If unsure, Funding Recipients should contact IRCC for guidance on how to dispose of personal client information.

Cloud storage services and servers

Cloud based services are not recommended for storing personal client information (Protected B). However, if a Funding Recipient must use cloud storage, the following should be considered:

- The cloud service provider’s datacentre must be physically located in Canada.
- If a Funding Recipient is using cloud services (ex., Dropbox or Google Drive) and the cloud service provider’s datacentre is not located in Canada, then no personal client information should be processed or stored.
- Canadian-based cloud service providers being used to process and store personal client information should conform to the **Government of Canada PBMM Cloud Profile**, which provides a set of security controls that are applicable to cloud-based applications.

Government of Canada PBMM Cloud Profile:

<https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html>

WI-FI

The use of Wi-Fi when inputting data into iCARE is acceptable if it is done using a trusted corporate or private Wi-Fi connection. A free public Wi-Fi connection, including free Wi-Fi at libraries, restaurant chains or any other free public Wi-Fi, should not be used to access the iCARE system.

Appendix B provides a checklist which can be consulted should a Funding Recipient offer Wi-Fi in the office.

Email

Electronic mail (email) is an integral part of doing business today. Funding Recipients have the responsibility and obligation under their CA to take steps to ensure that personal client information is not shared on unsecure networks. **The most secure approach is not to share personal client information (protected B) through email.**

In fact, when dealing with iCARE specific matters, personal client information should never be shared with IRCC using email. If personal client information needs to be shared with the iCARE team, it should be done using the telephone or iCARE secure message where available. If unsure, a Funding Recipient should contact IRCC for guidance on how to share personal client information.

If a Funding Recipient needs to share personal client information, and if there are no other methods to share this information, Funding Recipients should take measures to ensure information is protected when using email.

Before sending protected information via email the sender must ensure that both his/her network, and the recipient's network, can safeguard the integrity and confidentiality of the personal client information contained in the email. If this cannot be ensured then encryption is recommended.

IRCC recommends that all personal client information regarding IRCC funded clients be encrypted whether this is for internal or external distribution if the network is not sufficiently secure. The purpose of encrypting a file is to ensure that it cannot be viewed by anyone other than the intended recipient(s).

In order to encrypt the information it is recommended that the personal client information be saved as a separate document (such as Word or Excel) which can then be encrypted and attached to the email. Note that both the sender and the

recipient must have the same encryption software for the message to be opened by the recipient. Funding Recipients must assess organizational needs and select encryption software that meets these needs as long as the product meets FIPs 140-2 level 3 requirements. Examples of such software are Entrust (which is the Government of Canada, including IRCC, approved solution for desktop encryption) and WinZip.

Intrusion Detection

An **Intrusion Detection System** (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. An IDS comes in a variety of “flavours” and approaches the goal of **detecting** suspicious traffic in different ways.

The IDS can be combined with a firewall device or software that watches for traffic patterns and identifies attempts at unauthorized access to a network. It collects information on the origin of the transmission and takes various forms of action ranging from terminating the connection to informing the system administrator that an intrusion into the system or a system breach is in progress. This is often very useful in preventing future penetrations or probes.

It is up to the Funding Recipient to assess operational needs in determining what type of IDS is required.

Content Inspection

The Content Inspection software is like virus detection software but in reverse. It will examine messages and allow only those that are from legitimate sources and in a correct format to pass through. Note that clean transmissions originating from protected machines can be corrupted as they pass through other devices on a network, such as servers. This means that these messages can be infected and used to propagate viruses to other machines or networks. Content inspection will detect malicious code hidden inside legitimate looking messages and will drop or quarantine them.

It is up to the Funding Recipient to assess operational needs to determine what type of content inspection software is required.

How to respond when a computer or IT system is infected with a virus or malware

In the event that a virus or malware has infected a Funding Recipient’s system the Funding Recipient staff persons/Executive Director are advised to proceed as follows:

- 1) Take immediate action to limit the infection:
 - If applicable, Funding Recipient should notify their IT/Security personnel of the infection;
 - Isolate the infected computer(s) by disconnecting it from the network and the internet. This action can prevent continued infection and possible loss of additional files and the spread of the infection on the network. This will also permit a complete assessment of the issues by the Funding Recipient.
- 2) Document the issues:
 - This includes identifying the actual virus or malware that is infecting the computer so that a solution may be explored by the Funding Recipient.
 - Take inventory of the type of information on the system (such as personal client information) and whether the system was used to access iCARE. Note that any exfiltration of data may constitute a privacy breach. Review Part VII of this manual and take appropriate action.
- 3) Notify iCARE helpdesk (iCARE-iEDEC@cic.gc.ca) and the local IRCC office of the infection.
 - iCARE staff will determine if further action is required to protect the iCARE system. This may include reviewing all data input from the Funding Recipient and limiting the Funding Recipient's access to iCARE until satisfied the system is cleansed of infection.
 - Local IRCC office will be responsible for coordinating any further action with IRCC National Headquarters, including coordination in the case of a privacy breach.
- 4) Take proper measures to ensure systems are secure
 - It is the Funding Recipient's responsibility to ensure that their systems are secure and backed up. It is up to the Funding Recipient to assess the situation and to determine what actions are required to secure their system. However, IRCC may request a report on actions taken by the Funding Recipient to assess their current security posture.

TIPS to Prevent further Infections:

- **Update and patch systems:** This is a requirement of the MSR checklist but should be repeated - updating software will take care of many vulnerabilities.
- **Use antivirus/anti malware software:** Once again, this is a requirement of the MSR checklist and is an important step to protecting a network. It's basic but using antivirus will protect from the most basic, well-known viruses by scanning a system against these viruses.
- **Make safe and secure backups:** Recipients should consider making backups using physical disk drives, at regular and frequent intervals. Ideally these back up files are to a drive that remains entirely disconnected from the network. This may help limit the impact of a virus or malware attack.



- **Educate Staff:** Personal vigilance is a key component of protection against malware. Basic cyber safety and awareness knowledge such as ensuring workers don't click on questionable links in email or open suspicious attachments can prevent intrusion. Funding Recipients should also ensure that employees don't have unnecessary access to parts of the network that aren't critical to their work. This may limit the spread of certain malware, such as ransomware, if hackers do get into a system.
- **Have Policies/processes in place:** Develop policies and/or processes which address virus or malware infection. Ensure staff are aware of these policies and/or procedures and what steps to take if they find an infected computer, who needs to be contacted and what to document.

Part IV: Physical Requirements

Background

IRCC has reviewed the risk of unauthorized access to personal client information with regards to the physical placement of facilities, including computers, at Funding Recipients' offices. Inadequate physical security could lead to unauthorized access to personal client information. For example, monitors located in areas with public access, offices with windows, etc., may not be positioned properly to prevent viewing by unauthorized persons (internal or external). These situations could impact the confidentiality of personal client information.

Minimum Physical Requirements

All Funding Recipients are expected to comply with the following minimum physical security requirements, as identified in the MSR checklist:

Computers must be clearly marked to identify that they contain sensitive or personal information. This can be achieved simply by affixing labels to computer terminals indicating them as iCARE accessible stations.

Protocols are in place regarding proper marking of the security levels for any documents utilized or printed by the organization that contain personal or sensitive information. The manner in which organizations choose to do this is at their discretion. For example, IRCC uses the labels Protected A, B or C to indicate the level of security attached to a document.

If data is inputted in an open-concept office area, precautions are taken to ensure that monitors cannot be viewed easily by unauthorized persons. This includes using privacy monitor screens, and having monitors faced away from windows or other public areas, in order to prevent unauthorized viewing.



Additional Physical Requirements:

Beyond the MSR checklist, the following physical security measures should be implemented:

Password protection

A password written down could be compromised and lead to accidental data disclosure. Users are not to display their username and password where they can be seen by unauthorized personnel, must not share them and should not leave their computers unattended while logged into iCARE.

Printing and Document Handling

Users may accidentally print or send sensitive iCARE files to internal users without a need-to-know, or to external destinations without proper encryption. A lack of policy enforcement could result in sensitive assets being compromised. All files and documents generated from the iCARE system, which contains personal client information, will be marked to identify their security designation to ensure all information is handled and stored according to security requirements.

Part V: User Requirements

Background

All Funding Recipients must comply with IRCC identified user security requirements when accessing iCARE or handling personal client information. These requirements ensure that all staff employed by Funding Recipients are equipped to protect personal client information.

Note that all Funding Recipient staff who handle personal client information of IRCC funded clients must have an iCARE account, whether they use the account or not. This ensures that all staff who handle this information will have undergone an IRCC approved user reliability assessment.

For details on how to set up an iCARE user account please see the *"How to create and maintain iCARE User Accounts"* manual found in the Resources tab in iCARE.

User Reliability Assessment

All staff that will access personal information of IRCC funded clients are required to have an iCARE account, and must undergo a reliability assessment by the Funding Recipient's ED or ED designate prior to requesting a "username" for access to



iCARE. This assessment involves a verification of a staff person's past reliability to determine future reliability in relation to protecting client information.

If volunteers are given access to, or are required to collect, personal information of IRCC funded clients they must undergo a reliability assessment including a criminal record check (or its equivalent). The assessment should be kept in the volunteer's personnel file. However, volunteers are not required to have an iCARE account unless if they input data into iCARE as part of their responsibilities.



Note: When completing a reliability assessment, EDs are required to use the "iCARE User Authorization and Reliability Assessment Form" (Appendix D). This form was designed as a facilitative tool for EDs and completed forms should be kept in the staff person's personnel file.

1. Obtaining Consent

Prior to completing a reliability assessment, an ED must ensure that:

- No collection of information for reliability assessment purposes is undertaken without consent.
- Inform individuals who do not consent to the checks that further consideration cannot be given to them, with regard to accessing personal information of IRCC funded clients or the iCARE system.

EDs will base their decision on document/reference checks as follows:

- A verification of documents/references or an ED's personal knowledge of the individual.
- The results of a valid criminal record check (CRC) or equivalent documentation.

2. The Criminal Record Check

A criminal record check (CRC) is required to handle personal information of IRCC funded clients. A CRC is considered valid for user reliability assessment purposes only if it has been issued within the last 10 years. Acceptable equivalents to a valid CRC are:

- A valid Canadian Permanent Resident card for those who have obtained permanent residence in the last 10 years; or
- A valid Canadian citizenship card/certificate for those who have obtained citizenship in the last 10 years.



If the staff person obtained Canadian citizenship or Canadian permanent residency status more than 10 years ago they cannot use these as equivalents. They will need to obtain a valid CRC.

If a staff person needs to obtain a new CRC (or police certificate) for the purpose of handling personal client information it **should be obtained in the country of residence**.

The following website provides guidance, by country, on 'how to get a police certificate (also known as a Criminal Record check or police check):

<http://www.cic.gc.ca/english/information/security/police-cert/index.asp>.

Note that a "Vulnerable Sector (VS) check" is not required by IRCC as part of the CRC.

In Canada, a CRC may be performed by either the local police station or the Civil Section of the Royal Canadian Mounted Police (RCMP), depending on which office has authority in the Funding Recipient's area. In addition, there are a number of websites which offer Canadian CRC solutions. If unsure, Funding Recipients should contact IRCC for guidance on how to obtain a CRC.



Note: The CRC (or police certificate) should be kept in a secure location in the staff person's personnel file. IRCC may request to view this document during a monitor of the Funding Recipient's activities.

The existence of a criminal record can be, but need not be, sufficient grounds to deny reliability status. A criminal record should be considered in light of the duties and tasks to be performed, the nature and frequency of the offence, and the passage of time.

The ED will need to determine:

- The person's attitude towards the unparoned offence(s) and the extent to which he or she has changed behaviour in this regard.
- The likely recurrence of similar offences and their potential effect on the individual's reliability.

The ED must not inquire about a criminal offence for which a pardon has been granted.

The results of a CRC for the reliability assessment process remain valid for a period of ten years from the date of issue.

3. Verification of Information

An ED's reliability assessment involves the verification of certain pieces of information and a CRC in order to assess a staff person's truthfulness, honesty, trustworthiness and reliability. ED's may only give their authorization once they have conducted a reliability assessment of the staff person and have determined that the person is reliable for the purpose of accessing personal client information both in and out of iCARE.

Verification of Personal, Educational and Employment Information and/or References

EDs must limit their verification of a staff person's personal, educational and employment information and/or references to the last five years. The verification of one or all of these elements contributes to the ED's assessment as to whether a staff person is reliable, honest and trustworthy.

See Appendix E for detailed information on documents that may be used for the reliability assessment.

4. The Reliability Assessment Decision

In arriving at a reliability assessment decision, the ED is expected to provide a fair and objective assessment that respects the rights of the individual. The question to be answered is whether the individual can be relied upon not to abuse the trust that might be accorded in giving them access to personal client information.

In other words, is there reasonable cause to believe that the individual might exploit assets and information for personal gain, fail to safeguard information and assets entrusted to him or her, or exhibit behaviour that would reflect negatively on their reliability? Such decisions involve an assessment of any risks attached to giving them access and a judgment of whether such risks are acceptable or not.

The decision by the ED that the risk is acceptable means that the staff person has received a positive determination regarding reliability status and may proceed with applying for an iCARE user account and username.

For details on how to set up an iCARE user account please see the *"How to create and maintain iCARE User Accounts"* manual found in the Resources tab in iCARE.

If the risk is not acceptable, the individual must not be authorized to apply for an iCARE account, which also means that they cannot handle personal client information for IRCC funded clients. In addition, the individual must be given the reasons for denial.



Note: Sub-contracts: EDs are responsible for completing reliability assessments of staff persons who have access to personal client information or who need to access iCARE and who work for organizations with which the Funding Recipient has sub-contracted. Alternatively, they may delegate the task to the head of that organization; however, they continue to be responsible for ensuring that the reliability assessments have been performed.

5. A Positive Reliability Assessment

A positive reliability assessment for the purpose of obtaining an iCARE account remains valid for **10 years** while a staff person is employed at the current Funding Recipient. However, the ED may update or revoke it at any time. Periodic updates during the 10 year period are encouraged. An update following the 10 year period involves only the completion of a new criminal record check.

Please note that the User Reliability Assessment does not confer any kind of federal government security status on the individual. It is to be used strictly for the purpose of obtaining an iCARE account and allowing the person to handle personal information of IRCC funded clients. This process is not intended to have any effect on the employment relationship between the individual and the Funding Recipient (See Appendix D for a copy of the iCARE User Reliability Assessment Form).

6. The Security Briefing

Once staff persons have received a positive reliability assessment, they must be informed, orally or in writing, of their responsibilities with respect to safeguarding personal information of IRCC funded clients through a comprehensive security awareness training program. Instructing staff to study the details of this manual would satisfy this requirement.

7. Completing the iCARE User Account Request Form

Once staff persons have received a positive reliability assessment and the security briefing outlined above, the ED and staff person can request an iCARE user account.

For details on how to request and set up an iCARE user account please see the "*How to create and maintain iCARE User Accounts*" manual found in the Resources tab in iCARE.

As part of the process the ED and staff person must complete the iCARE User Account Request Form. Checking the two security boxes on the form indicates that the staff person agree to abide by the iCARE User Security Requirements. Copies of these forms and the CRC should be stored in the staff person's personnel file.





Note: The ED's and staff person's signatures on the iCARE User Authorization and Reliability Assessment Form are retained as attestation to the deliverance of the security briefing.

8. Cancelling an iCARE Account

When a staff person's reliability assessment has been revoked or there is a request for a cancellation of an iCARE account (for example when an employee retires or leaves for other employment), the ED will deactivate the account through the User Account Request page in iCARE. As soon as the ED saves the record in iCARE, the user's account is deactivated. (Details on the process for deactivating a user account are included in the *"How to Create and Maintain iCARE User Accounts"* Manual.)

Note: Only IRCC can deactivate an ED's or Organization's account.

Reliability Assessment Records

Retention

EDs are required to keep a copy of the staff person's criminal record check certificate or equivalent for IRCC monitoring purposes.

Disposal

Any records relating to the reliability assessment must be destroyed two years from the date the staff person ends employment.

Access

Any records relating to the reliability assessment are to be used only for the purposes for which they were collected and must not be disclosed to anyone (with the exception of IRCC) without the staff person's consent.

User Requirements Checklist

All users of iCARE must be aware of and abide by the following security requirements:

- Only individuals with an iCARE username and password are allowed to access iCARE.
- Users must keep their username and password confidential at all times, i.e., they are never to disclose them, display them where they can be viewed, or share them with anyone.



- Client information in iCARE is sensitive information and users must keep it confidential at all times in accordance with privacy provisions in the IRCC Contribution Agreement.
- Users are not to leave their computers unattended while logged into iCARE or inputting personal client information.
- Users are to immediately report all attempts or occurrences involving unauthorized access to iCARE or iCARE client information being altered, damaged or stolen to the Funding Recipient ED who must immediately report this to the IRCC Officer who manages the Contribution Agreement.
- Users who no longer require access to iCARE have a continuing obligation to maintain the confidentiality of the personal client information to which they have had access.
- IRCC site visits, reviews and/or audits may be conducted at any time, and iCARE usernames and passwords may be revoked at any time.

Part VI: Organizational Security Policies and Training

Background

In accordance with the MSR checklist, it is imperative that Funding Recipients comply with the organizational security policies required by IRCC. The security requirements in this category emphasize the importance of training and policy procedures that all Funding Recipients should have in place when dealing with personal client information.

Training Requirements

- Funding Recipients are responsible for providing staff with a comprehensive security awareness training;
- Funding Recipients must ensure that internal security training is reviewed and changed, as necessary, when updates in security requirements occur.

Procedures and Policies

Funding Recipients must have the following policies, procedures and/or safeguards in place in order to collect personal client information:

- There is a procedure and/or policy in place to ensure that individuals keep their username and password confidential at all times;
- There are safeguards in place to ensure that only individuals with an iCARE account are allowed to access iCARE;



- There is an iCARE account creation procedure which includes the user reliability assessment and the privacy/security briefing, including obtaining a Criminal Record Check or it's equivalent;
- There is a procedure in place for prompt removal of iCARE network access upon employee termination;
- There is a procedure in place to limit the collection of personal information to only that which is necessary to carry out IRCC programming or meet operational requirements;
- There is a procedure in place for ensuring that all employees use and interaction with personal client information is audited or monitored;
- There is a policy and procedure in place for the safe, secure and documented disposition of personal client information;
- There is a policy and procedure in place for providing clients with reasonable access to their own personal information collected as part of the Settlement and Resettlement Programs;
- There are policies and /or procedures in place to ensure that client information is handled pursuant to applicable legislation and regulations governing personal information as identified in section 7 of the contribution agreement. See Appendix C for an example of a Handling of Sensitive Material protocol.

Part VII: Privacy Breaches and Violations

Background

Privacy and Security are important parts of the work Funding Recipients undertake. If a privacy violation or breach is suspected or has occurred that may affect the security of personal information of IRCC funded clients, staff persons should immediately notify the ED of the organization. The purpose of this section is to provide guidance to IRCC's Funding Recipients for situations when a privacy breach involving personal client information is suspected or has occurred.

Term	Definition
Privacy breach	A privacy breach involves improper or unauthorized collection, use, disclosure, retention and/or disposal of personal information. A breach may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.



Term	Definition
Privacy violation	<p>Events that could have led to a privacy breach but did not.</p> <p>These events may involve a threat arriving over the Internet, such as a virus or hacker, or unauthorized persons attempting to gain access to personal client information.</p>

Privacy Breaches – Guidance for Funding Recipients

Potential Causes of Privacy Breaches

The following are examples of situations that could result in the disclosure of or access to personal client information by unauthorized parties.

- The theft, loss or disappearance of equipment or devices containing personal client information.
- The sale or disposal of equipment or devices containing personal client information without a total purging of the item prior to its sale or disposal.
- The transfer of equipment or devices without adequate security measures.
- The use of equipment or devices to transport/store personal client information outside the office for tele-work or off-site work arrangements without adequate security measures.
- The inappropriate use of electronic devices to transmit personal client information, including telecommunication devices.
- Intrusions that result in unauthorized access to personal client information.
- Low level of privacy awareness among staff, contractors or other third parties that handle personal client information.
- Inadequate security and access controls for information in hard copy or electronic format, on-site or off-site.
- The absence of or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal client information.
- Insufficient measures to control access and editing rights to personal client information. This may result in wrongful access to and the possible tampering of records containing personal client information.

How to Respond to a Privacy Breach

In the event that a privacy breach is suspected or has occurred, the Funding Recipient must immediately notify the IRCC officer responsible for managing the agreement. The organization may be required to work with IRCC staff to investigate



and provide as much specific and detailed information as possible to fully explain the breach.

The Funding Recipient should also refer to the applicable privacy law for the jurisdiction where the breach occurred, e.g. municipal, provincial, country, to determine if there are any additional reporting requirements with respect to breaches of privacy. Information on responding to privacy breaches can be found from the appropriate provincial/territorial agency, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or the country where the breach occurred. Information dealing with privacy breaches can also be found on the Office of the Privacy Commissioner of Canada (OPC) website: www.priv.gc.ca . If the personal information was collected from clients outside of Canada, please note that the privacy laws of that country may apply.

Should a privacy breach occur concerning IRCC funded client information, the Funding Recipient staff persons/Executive Director must proceed as follows:

1. Take immediate action to stop the breach and to secure the affected records, systems or user access:
 - Remove, move or segregate exposed information/files. That is, take necessary action to prevent further wrongful access.
 - In some cases, it may be necessary to shut down access to the iCARE system, application or device temporarily to permit a complete assessment of the breach and resolve vulnerabilities.
 - Attempt to retrieve any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person.
 - Return the documents to their original location or to the intended recipient unless its retention is necessary for evidentiary purposes.
2. Document the privacy breach:
 - Document in detail the circumstances that gave rise to the privacy breach.
 - Take inventory of the personal information that was or may have been compromised.
 - Identify the parties whose personal information has been wrongfully disclosed or accessed, stolen or lost.
 - Identify the organizational sector or third party that is responsible for the personal information involved.
 - Include other relevant information (ex: previous similar or related incidents).



Note: The organization should make reasonable efforts to identify the individuals affected by the breach. If this is not possible, efforts should be made to identify the

groups of individuals likely to have been affected. The organization should also document the process that it carries out to identify affected individuals.

2. Notify Local IRCC office of the privacy breach:

- As per section 7 of the CA, Funding Recipients will need to contact the local IRCC office responsible for administering the CA to inform them of the breach and provide them with all pertinent information collected as identified above.
- This IRCC office should be kept informed at regular intervals and of the final outcome whenever an investigation is conducted.
- The IRCC local office is responsible for coordinating any further action with IRCC National Headquarters.



Appendix A - iCARE Minimum Security Requirements



iCARE MINIMUM SECURITY REQUIREMENTS

Organization Name:

SECURITY ITEM	YES	NO	CLIENT RESPONSE (if answer is "No", please specify steps that will be taken to address requirement)
Technological Security Requirements			
1	<input type="checkbox"/>	<input type="checkbox"/>	
2	<input type="checkbox"/>	<input type="checkbox"/>	
3	<input type="checkbox"/>	<input type="checkbox"/>	
4	<input type="checkbox"/>	<input type="checkbox"/>	
5	<input type="checkbox"/>	<input type="checkbox"/>	
Physical Requirements			
6	<input type="checkbox"/>	<input type="checkbox"/>	
7	<input type="checkbox"/>	<input type="checkbox"/>	
8	<input type="checkbox"/>	<input type="checkbox"/>	
User Requirements			
9	<input type="checkbox"/>	<input type="checkbox"/>	
10	<input type="checkbox"/>	<input type="checkbox"/>	
11	<input type="checkbox"/>	<input type="checkbox"/>	
12	<input type="checkbox"/>	<input type="checkbox"/>	



Organization Name:

	SECURITY ITEM	YES	NO	CLIENT RESPONSE (If answer is "No", please specify steps that will be taken to address requirement)
Organizational Security Policies and Training				
13	There is a procedure and/or a policy in place to ensure that individuals keep their username and password confidential at all times (i.e. they are never to disclose them, display them where they can be viewed, or share them with anyone)	<input type="checkbox"/>	<input type="checkbox"/>	
14	Your organization has an ICARE account creation procedure: <ul style="list-style-type: none"> • User Reliability form completed; • Privacy/Security Briefing completed; • User Account Request Form (pdf) completed and submitted with Criminal Records Check (or equivalent) through ICARE and copies retained on personnel file; • User Reliability Assessment form signed and copy retained on personnel file. 	<input type="checkbox"/>	<input type="checkbox"/>	
15	Your organization has a procedure for prompt removal of ICARE network access upon employee termination	<input type="checkbox"/>	<input type="checkbox"/>	
16	There are safeguards in place to ensure that ONLY individuals with an ICARE account are allowed to access ICARE	<input type="checkbox"/>	<input type="checkbox"/>	
17	There is a comprehensive security awareness training program available and provided to all staff (Instructing staff to study the details of the ICARE Security Requirements manual would apply)	<input type="checkbox"/>	<input type="checkbox"/>	
18	Your internal security training is reviewed and changed, as necessary, when updates in security requirements occur	<input type="checkbox"/>	<input type="checkbox"/>	
19	Staff that require access to ICARE undergo a police criminal records check* (CRC's) as a condition of employment with your organization (*includes valid CRC's, Citizenship card and Permanent Resident card)	<input type="checkbox"/>	<input type="checkbox"/>	
20	Your organization currently has procedures in place to audit or monitor employees' use and interaction with sensitive information	<input type="checkbox"/>	<input type="checkbox"/>	
21	Your organization currently has a policy in place for safe, secure and documented disposition of client information	<input type="checkbox"/>	<input type="checkbox"/>	
22	Your organization currently has policies and/or procedures in place to limit the collection of personal information to only that which is necessary to carry out ICARE programming	<input type="checkbox"/>	<input type="checkbox"/>	
23	Your organization currently has policies and/or procedures in place to provide clients with reasonable access to their own personal information collected as part of the ICARE program	<input type="checkbox"/>	<input type="checkbox"/>	
24	Your organization currently has policies and/or procedures in place to ensure that client information is handled pursuant to applicable legislation and regulations governing personal information	<input type="checkbox"/>	<input type="checkbox"/>	

IMM 5758 (02-2016) E



Appendix B – Wireless Recommendations

Should a Funding Recipient choose to offer Wi-Fi in the office the implementation of the following safeguards could improve the security and operational efficiency of the environment so that systems could operate in a suitably secure fashion.

- Provide training to staff on how to access the wireless network and safeguard information on portable devices
- Limit the range of the network coverage to the immediate vicinity of the Office
- Do not broadcast wireless network SSID
- Do not use default SSID
- Use WPA2
- Use 802.1X server-based authentication
- Change the key frequently
- Use a VPN and Firewall to isolate the WLAN
- Use a personal firewall on every wireless client
- Install wireless intrusion detection/prevention systems
- Document and enforce a complex password schema for WPA2 pass-phrase/key
 - I. Minimum 8 characters
 - II. At least one upper case character
 - III. At least one lower case character
 - IV. At least one number
 - V. At least one special character (@#\$%&?><:;/~!)
 - VI. Not a dictionary word
 - VII. Not a person, place, or pet name
- Monitor logs for bad logon attempts and double MAC address access attempts
- Physically secure access to wireless network hardware (i.e.: WAP, Radius, etc.)
- Harden WAP devices to not permit cross-device communication. Only communication with the WAP is permitted.
- When a wireless device has both an Ethernet connection and Wi-Fi connection, ensure a policy exists to only permit one to function at a time, and a wired connection (when present) overwrites and disables the wireless connection.
- Harden domain connected wireless devices to only permit access to the Wi-Fi network, and all other network connections on the device is restricted. No access is permitted through external Wi-Fi or Ethernet connections.
- Users must turn off wireless devices with a voice transmission capability when attending a meeting at which sensitive information, above Protected A, is being shared.
- Limit and filter internet and network access prior to user authentication against corporate networks.

Appendix C: Example of a Protocol for Handling Sensitive Material

Item	Description
Protected A	Indicates a low level of sensitivity and is normally added to records that contain, for example, limited amount of personal information about a client or information that does not reveal many facts about the client. A document containing the name and home address of a client would fall under this category.
Document Marking	All pages on top right-hand corner: PROTECTED A
Communication	Use a regular telephone, regular mail and email
Packaging	Use a single envelope with no security marking Deliver by hand, internal or first-class mail
Protected B	Used to identify information that is “particularly sensitive”, and applies to client information that Funding Recipients commonly handle – when tombstone information is combined with settlement/resettlement service information it would be classified as Protected B.
Document Marking	All pages on top right-hand corner: PROTECTED B

Item	Description
Communication	Use a regular telephone, mail and a secure fax Use discretion on cellular telephone Email can only be used if on secure network or if encrypted
Packaging	Use a single envelope marked with "To be opened by addressee only" Deliver by hand, internal or first-class mail.

Appendix D – iCARE User Reliability Assessment Form

This is an internal form to be used in determining the reliability of a person who will access personal information of IRCC funded clients.

iCARE User Reliability Assessment Form			
<input type="checkbox"/> New <input type="checkbox"/> Update			
PART A TO BE COMPLETED BY THE USER			
Surname:		Full given names (no initials) <u>underline name used</u> :	
Family name at birth:		All other names used:	
Date of Birth:	Sex:	Telephone number:	
Y-A M-M D-J 	<input type="checkbox"/> Male <input type="checkbox"/> Female	Home: () Work: ()	
Home Address:		City/Town:	Province:
			Postal Code:
PART B PARTICULARS OF POSITION			
Position Title:			
PART C RELIABILITY ASSESSMENT AND CONSENT			
NOTE: Unless cancelled in writing by the individual, this consent form shall be valid for conducting the checks specified below, as well as for subsequent updating requirements.			
_____		_____	
Individual's Signature		Date	

<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Employment History		
<input type="checkbox"/> Address	<input type="checkbox"/> References		
<input type="checkbox"/> Education / Professional Qualifications	<input type="checkbox"/> Criminal Record Check - Please include: Certificate Number: Date of Issue: Authority:		
I, the undersigned, confirm having received an oral or written briefing on the iCARE User Security Requirements and I agree to respect them for as long as I have access to iCARE, and after my access is terminated.			
_____ Individual's Signature		_____ Date	
I, the undersigned, as the Service Provider Organization (SPO) Executive Director (E.D.) or designate, do hereby certify that the above information has been verified. In accordance with the 'iCARE Security Requirements for Service Provider Organizations', I consider this individual to be reliable for the purposes of accessing iCARE.			
_____ Signature		_____ Date	
Name and title of authorized official:	Office Address:	Telephone:	Facsimile:
		()	()



Appendix E: iCARE User Reliability Assessment Table

User information to verify	Purpose of verification	Examples of what to verify
Part A		
Date of Birth (i.e., personal data)	To ensure that the identity of the person being checked is bona fide.	<ul style="list-style-type: none"> • Birth certificate • Other verifiable official document
Address (i.e., personal data)	Same as above.	<ul style="list-style-type: none"> • Driver's license • Lease or other verifiable official document
Education and professional qualifications	To ensure that the individual is being truthful about background and history.	<ul style="list-style-type: none"> • Education/professional certificate • Other official document from educational institution, e.g., letter
Employment history	To determine whether the individual has been reliable and to ensure that the individual is being truthful about background and history.	<ul style="list-style-type: none"> • Contact with previous employers
References/personal character	To determine whether the individual has been honest, trustworthy, and reliable. This does not include a credit check.	<ul style="list-style-type: none"> • To be limited to references provided by individual



Part B		
A Criminal Record Check (Police Certificate/ Police Check)	To determine whether the user has in the past committed crimes that may indicate an unacceptable risk in relation to giving them access to personal client information.	<ul style="list-style-type: none"> To be obtained by individual from their country of residence.
Instead of a new criminal record check you can submit:		
Copy of existing Criminal Record Check	Persons who have obtained a criminal record check (CRC) within the last 10 years, can submit a copy of this CRC.	
Copy of valid Canadian Permanent Resident card	Persons who became Canadian Permanent Residents within the last 10 years can submit a copy of their valid PR card in lieu of a criminal record check.	
Canadian Citizenship card/certificate	Persons who became Canadian Citizens within the last 10 years can submit a copy of their Canadian Citizenship card/certificate in lieu of a criminal record check.	