



Immigration-Contribution Accountability Measurement System



Security Requirements for Service Provider Organizations

November 2002

TABLE OF CONTENTS

Executive Summary

Introduction

PART I: User Security

1. The reliability assessment

- 1.1 Background
- 1.2 Verification of information
- 1.3 Exemptions
- 1.4 Conflict of interest
- 1.5 Validity, updating and revoking
- 1.6 Sub-contracts

2. Processing reliability assessment information

- 2.1 User consent
- 2.2 Verification of personal, educational and employment information and/or references
- 2.3 Verification of the criminal records check results
- 2.4 Completing the *'iCAMS User Authorization and Reliability Assessment Form'* (optional)

3. The reliability assessment decision

4. A positive reliability assessment

- 4.1 The security briefing
- 4.2 Completing the *'iCAMS Username and Password Request/Update Form'* (mandatory)

5. Reliability assessment records

- 5.1 Retention, disposal and access

6. Cancelling an iCAMS Username and Password

- 6.1 Completing the *'iCAMS Username and Password Cancellation Form'*

PART II: IT Security

- 1. Background**
- 2. The iCAMS environment**
- 3. Requirements: Stand-alone (non-networked) computers accessing iCAMS**
- 4. Recommendations: Networks and networked computers**

PART III: Physical Security

- 1. Background**
- 2. Requirements**

PART IV: Security Breaches and Violations

Appendices

Appendix A – Guidance

Appendix B – *iCAMS User Authorization and Reliability Assessment Form*

Appendix C – iCAMS User Security Requirements

Appendix D – *iCAMS Username and Password Request/Update Form*

Appendix E – *iCAMS Username and Password Cancellation Form*

Appendix F – Feedback Form *iCAMS Security Requirements for Service Provider Organizations*

Executive Summary

In 1999, Citizenship and Immigration Canada (CIC) developed the Contribution Accountability Framework (CAF) for contribution programs. These programs include the Language Instruction for Newcomers to Canada (LINC) Program, the Immigrant Settlement and Adaptation Program (ISAP), the Host Program, and the Resettlement Assistance Program (RAP). The Immigration-Contribution Accountability Measurement System (iCAMS) was designed to support the performance measurement component of CAF. iCAMS is an Internet-based system that collects client and service data from Service Provider Organizations (SPOs) receiving contribution funding. The information collected will allow SPOs and CIC to provide better services to clients, increase program effectiveness, and show the public that funds are being spent responsibly.

The client information collected in iCAMS is equivalent to designated information in the federal government that is also "particular sensitive", that is, its disclosure would reasonably be expected to cause serious injury to the individuals concerned, and minimum safeguards must be in place to protect it.

CIC is required to protect personal client information under federal privacy legislation. This requirement is extended to SPOs through the contribution agreement. In developing iCAMS, CIC was advised by internal and external privacy and security experts that, because it is an Internet-based system and because of the quantity of client information it contains, specific security measures must be introduced to protect the information. CIC, therefore, has an obligation to articulate clear security measures for the iCAMS environment. These security measures are outlined in this document and include user, technological and physical security **requirements**. CIC is also making a series of **recommendations** that will be left up to the discretion of the SPO to implement. CIC would encourage SPOs and their Boards of Directors (if Boards exist) to implement any additional policies and procedures they deem necessary to protect clients and their personal information.

User Security Requirements:

- CIC requires all users to obtain a "username" and "password" to access iCAMS. Prior to being provided with these, SPO users (including employees and volunteers) must undergo a reliability assessment and be found to be reliable by the Executive Director (E.D.) or a designate. The reliability assessment is comparable to the federal government's "enhanced reliability check" and will be based on a) a verification of documents/references **or** an E.D.'s personal knowledge of the individual; and b) the results of a criminal records check.
- Note: long time employees of a SPO, persons who have already obtained a criminal records check at a SPO or persons employed at a SPO who became permanent residents within the year preceding their application for a username and password are exempted from the requirement to undergo a reliability assessment.

Technological Security Requirements:

- In order to protect client information in iCAMS from external threats, such as those arriving over the Internet, and from internal threats, such as unauthorized access, CIC is requiring SPOs to install an anti-virus and firewall software package (McAfee VirusScan 7 or equivalent) on all stand-alone computers accessing iCAMS. Users are also required to install a log-in password and a password-protected screen-saver.
- CIC is also **recommending** that anti-virus and firewall protection be installed on networks in order to protect networked computers.

Physical Security Requirements:

- CIC is requiring users to take minimal precautions in terms of preventing access to iCAMS by unauthorized persons. These include ensuring that computer monitors are turned away from public access areas and windows while iCAMS is being used. It also includes ensuring that usernames and passwords are not displayed where they can be seen by unauthorized personnel, that they are not shared with anyone and that computers are not left unattended while logged into iCAMS.

The security requirements outlined in this document will be part of the CIC contribution agreement with SPOs. CIC will provide **one-time** start-up compensation to cover such costs as the criminal record checks for identified iCAMS users, McAfee software for computers accessing iCAMS, and the time to train users. Additional ongoing costs associated with these requirements may be negotiated with the local CIC offices. There will be a **six month phase-in period** from the time SPOs are formally trained on iCAMS-LINC, ISAP and Host to the time they will be expected to have completed the implementation of these requirements. The phase-in period for SPOs offering RAP will last until the signing of their next contribution agreement, or April 1, 2003 if they are signing new agreements in January 2003.

A feedback form for completion by SPOs is provided at the end of this document in order to obtain comments on the security requirements. The feedback received will be used to determine if any changes need to be made.

Guidance or assistance on these requirements may be obtained from the members of the CIC Contribution Accountability Team as provided in **Appendix A**.

Introduction

In 1999, Citizenship and Immigration Canada (CIC) launched the development of the Contribution Accountability Framework (CAF) for its settlement and re-settlement contributions programs. These comprise the Language Instruction for Newcomers to Canada (LINC) Program, the Immigrant Settlement and Adaptation Program (ISAP), the Host Program, and the Resettlement Assistance Program (RAP). The purpose of the CAF is to ensure the accountability of departmental expenditures, the monitoring of service delivery and the evaluation of the effectiveness of contribution programs in meeting the settlement needs of newcomers. CAF has the following five components:


- Evaluation
- Performance Measurement
- Contribution Agreement Process
- Management Control Framework
- Provincial/Territorial Accountability

CIC has focused on the performance measurement component since 2000, which has involved the development of the Immigration – Contribution Accountability Measurement System (iCAMS) in collaboration with Service Provider Organizations (SPOs) that receive contribution funding. iCAMS is an Internet-based system designed to collect performance measurement data. It will allow SPOs to provide consistent and reliable program data to CIC. This information will assist SPOs and CIC in providing better services to clients, increasing program effectiveness, and showing the public that funds are being spent responsibly. Together with the implementation of the other components of CAF, CIC should be well-positioned to report on results being attained.


iCAMS is collecting individual client information for LINC and RAP and aggregate or individual (optional) client information for ISAP and Host. Information collected includes a client's name, birth date, immigration number and services received. Because of its type (i.e., personal information) and quantity, the information in iCAMS is equivalent to federal government "designated" information that is also "particularly sensitive", which means that its disclosure would reasonably be expected to cause serious injury to the individuals concerned. It must, therefore, be safeguarded according to certain minimum standards.

CIC is required to protect personal client information under federal privacy legislation. This requirement is extended to SPOs through the contribution agreement. In order to ensure the protection of the client information in iCAMS and as part of the development process of an Internet-based system, CIC conducted a number of privacy and security assessments. These included a Threat and Risk Assessment and a Privacy Impact Assessment (a summary is available on www.integration-net.cic.gc.ca).


CIC also consulted on these issues with the Office of the Privacy Commissioner of Canada, external partners and with internal departmental specialists. CIC was advised that in order to meet its obligations under federal privacy legislation, specific security requirements should be introduced for the iCAMS environment. These requirements are outlined in this document and include personnel, technological and physical security measures. They are based on current federal government privacy and security policy and are designed to protect client information in iCAMS and SPO databases. It should be noted that the adoption of these types of measures is good practice for any environment where personal information is collected and stored.

 **Part 1** of the document outlines the personnel or user security requirements. All users will be required to undergo a reliability assessment by the SPO Executive Director (E.D.) or a designate prior to requesting a “username” and “password” for access to iCAMS. This assessment is comparable to the federal government’s “enhanced reliability check” and involves a verification of a user’s past reliability to determine future reliability in relation to protecting client information in iCAMS. E.D.s will base their decision on document/reference checks or their personal knowledge of the individual and the results of a criminal records check. Users who receive a positive reliability assessment may apply for access to iCAMS.

The assessment does not confer any kind of federal government security status on the individual. It is to be used strictly for the purpose of accessing iCAMS and is not intended to have any effect on the employment relationship between the individual and the SPO.

 **Parts II and III** of this document discuss the requirements related to technological and physical security, respectively. Technological security refers to security measures that are designed to protect information from external threats, such as those arriving over the Internet and from internal threats, such as from individuals seeking unauthorized access.

Recommendations to enhance technological security are also provided in this part. Physical security involves the proper layout and design of facilities and the use of measures to prevent unauthorized access.

 **Part IV** discusses the action to be taken by the E.D. and/or users in the event of a security breach or violation at a SPO that could affect the security of client information in iCAMS.

SPOs are required to implement these security requirements under the CIC contribution agreement as part of the process of collecting client information for iCAMS. Guidance or assistance on their implementation may be obtained from the members of the CIC Contribution Accountability Team as provided in **Appendix A**.

PART I: User Security

1. The user reliability assessment

1.1 Background

CIC is providing SPO users (employees and volunteers) with username and passwords on a “need-to-know” basis and with the authorization of the Executive Director (E.D.) or a person designated by the E.D. (references to “E.D.” in this document will include the designate). The term “users” in this document refers to both persons applying for and holders of a username and password. E.D.’s may only give their authorization once they have conducted a reliability assessment of the user (exceptions are given in section 1.3) and have determined that the person is reliable for the purpose of accessing client information in iCAMS.

1.2 Verification of information

An E.D.’s reliability assessment involves the verification of certain pieces of information and a criminal records check in order to assess a user’s truthfulness, honesty, trustworthiness and reliability. *Part A* of the table below is provided as a guide in deciding what information (other than the criminal records check results) to verify when making an assessment. Instead of verifying one or more pieces of this information, E.D.s may choose to rely on their **personal knowledge** of the individual. It is mandatory, however, that they consider the results of a criminal records check (*Part B* of the table) when making their reliability assessment decision.

iCAMS 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 licence • 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. This does not include a credit check.	<ul style="list-style-type: none"> Contact with previous employers
References/personal character	To determine whether the individual has been honest, trustworthy, and reliable.	<ul style="list-style-type: none"> To be limited to references provided by individual
Part B		
A check of criminal records	To determine whether the user has in the past committed crimes that may indicate an unacceptable risk in relation to giving them access to client information in iCAMS.	<ul style="list-style-type: none"> To be obtained by individual from local police office or RCMP

1.3 Exemptions

The following describes the situations in which persons, who have otherwise been authorized by the E.D. to apply for a username and password, are exempt from the requirement to undergo a reliability assessment (E.D.s may chose to conduct one in any event):

- Persons who have been employed with a SPO for a period of at least **three years**.
- Persons employed at the SPO who underwent criminality and security background checks as part of an application for permanent residence and who became permanent residents within the year preceding their application for a username and password.
- Persons who, for the purpose of employment or while employed at a SPO, completed a criminal records check under:
 - ✓ internal SPO security policy
 - ✓ the security policy of other funders/partners or,
 - ✓ federal/provincial/municipal security legislation
- Existing users, who become employed at a different SPO, are required to apply for a new username and password but are not required to undergo a reliability assessment.

1.4 Conflict of Interest

E.D.s must not perform their own reliability check.

1.5 Validity, updating and revoking

A positive reliability assessment for the purpose of obtaining a username and password remains valid for **10 years** while a user is employed at the current or another SPO; however, the E.D. may update or revoke it at any time. An update involves only the assessment of new criminal records check results.

1.6 Sub-contracts

E.D.s are responsible for completing reliability assessments of users working for organizations with which the SPO has sub-contracted. Alternatively they may delegate the task to the head of that organization.

2. Processing reliability assessment information

2.1 Obtaining consent

E.D.s must:

- ✓ Ensure that no collection of information for reliability assessment purposes is undertaken without the consent of the person concerned.
- ✓ Inform individuals who do not consent to the checks that further consideration cannot be given to them accessing iCAMS.

2.2 Verification of personal, educational and employment information and/or references

E.D.s must limit their verification of a user's personal, educational and employment information and/or references (i.e., the elements in Part A of the iCAMS User Reliability Assessment Table) to the last **five years**. The verification of one or all of these elements contributes to the E.D.'s assessment as to whether a user is reliable, honest and trustworthy.

2.3 The criminal records check

A criminal records check is 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 SPO area. A certificate indicating the results will be issued.

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 E.D. will need to determine:

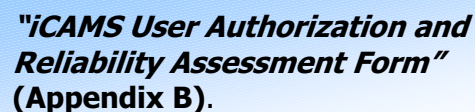
- The person's attitude towards the unpardoned offence(s) and the extent to which he or she has changed behaviour in this regard.
- The likely recurrence of similar offences and their potential effect on the individual's reliability.

The E.D. must not inquire about a criminal offence for which a **pardon** has been granted.

The results of a criminal records check for the iCAMS reliability assessment process remain valid for a period of **twelve** months after the date of issue.

2.4 Completing the "iCAMS User Authorization and Reliability Assessment Form"

When completing a reliability assessment, E.D.s may use the:



"iCAMS User Authorization and Reliability Assessment Form"
(Appendix B).

This form was designed as a facilitative tool for E.D.s and its completion is optional.

3. The reliability assessment decision

In arriving at a reliability assessment decision, the E.D. 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 client information in iCAMS.

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 judgement of whether such risks are acceptable or not.

The decision by the E.D. that the risk is acceptable means that the user has received a positive determination regarding reliability status and may proceed with applying for a username and password as described in the next section.

If the risk is not acceptable, the individual must not be authorized to apply for a username and password. In addition, the individual must be given the reasons for denial.

4. A positive reliability assessment

4.1 The security briefing

Once users have received a positive reliability assessment, they must be informed, orally or in writing, of their responsibilities with respect to safeguarding iCAMS client information in accordance with the:

"iCAMS User Security Requirements"
(Appendix C).

These requirements include notifying the E.D. when unauthorized access to iCAMS is sought or when iCAMS client information is altered, damaged or stolen. The E.D. must immediately forward all information concerning these types of incidences to a member of the CIC Contribution Accountability Team (see Appendix A).

4.2 Completing the *"iCAMS Username and Password Request/Update Form"*

Once users have received a positive reliability assessment and the security briefing outlined above, the E.D. and user must sign the:

"iCAMS Username and Password Request/Update Form"
(Appendix D).

The E.D.'s signature authorizes the user to apply for a username and password while the user's signature indicates that they agree to abide by the iCAMS User Security Requirements.

5. Reliability assessment records

5.1 Retention, disposal and access

Retention:

E.D.s are required to keep a record of the number, the date of issue and issuing authority of the user's criminal records check certificate for CIC monitoring purposes.

Disposal:

Any records relating to the reliability assessment must be destroyed two years from the date the user 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 the criminal records check certificate number, date of issue and authority, which may be provided to CIC) without the user's consent.

6. Cancelling an iCAMS Username and Password

6.1 Completing the '*iCAMS Username and Password Cancellation Form*'

When a user's reliability assessment has been revoked or there is a request for a cancellation of a "username" and "password", the E.D. and the user must sign the:

***"iCAMS Username and Password
Cancellation Form" (Appendix E).***

The E.D.'s signature authorizes the request for a cancellation of the user's username and password while the user's signature indicates that they understand their continuing commitment to protect the iCAMS client information to which they have had access.

PART II: IT Security Requirements and Recommendations

1. Background

Information technology (IT) security is intended to ensure the confidentiality and integrity of information stored, processed or transmitted electronically. The federal government adopts various security measures, as required by RCMP, Treasury Board, and departmental IT security policies, to protect its electronic systems. At CIC, for example, security measures are employed at various system levels, such as at the network perimeter (where the rest of the world connects to CIC) and within the network itself, such as at the individual desktop level. Security measures include, as a minimum, firewall and anti-virus software. Brief descriptions of these are provided below.

Firewalls: These may be used at both the network and individual workstation level. They 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.

Virus scanning: This may also be used at various system levels (i.e., at the network and individual computer level) to ensure that all traffic arriving at these areas is processed by a virus scanning engine that examines messages or transmissions in order to detect virus codes. If the message or transmission is safe, it is passed to the recipient. If it is not, it is rejected or quarantined. It should be noted that in the case of networked computers, where only the computers are equipped with anti-virus software, clean transmissions originating from these machines can be corrupted as they pass through other devices on the network, such as the servers. This means that the message could be infected and used to propagate the virus to other machines or networks. In addition, a protected computer connected to a network that has been corrupted is useless, as it will not be able to access anything on the network.

2. The iCAMS environment

CIC is implementing IT security requirements and making recommendations for the iCAMS environment at SPOs to ensure that all transmissions to the iCAMS database are safe (i.e., free from malicious code such as viruses, that may have been acquired by the SPO and inadvertently transmitted onward).

They are also intended to protect SPO databases, files and e-mail traffic from threats arriving over the Internet.

2.1 Requirements: Stand-alone (non-networked) computers accessing iCAMS

These requirements apply to stand-alone computers (not connected to a network) through which iCAMS is accessed. SPOs are required to:

1. Install McAfee VirusScan 7.0, which is a firewall and anti-virus protection software package, on all stand-alone iCAMS computers.

The CIC IT Security Division has advised that while no software is able to guarantee that a system will not be compromised, the recommended package should provide a reasonable amount of protection.

SPOs may use an alternate product as long as the security features are comparable to McAfee VirusScan 7.0.

Note that virus protection software requires regular **updating** (which can be weekly) in order to effectively detect new viruses. The instructions on installing the software package will explain how to do this.

Further information on McAfee VirusScan 7.0 can be obtained at the following website: <http://www.mcafee.com/myapps/vs7/>

For added security, we require that each user install on stand-alone computers through which iCAMS will be accessed:

- 2. a log-in password (to be changed periodically), and**
- 3. a screen-saver with password protection (an activation period of no more than 15 minutes of non-usage is suggested)**

2.2 Recommendations: Networks and networked computers

In the case of computers connected through a network, it is ineffectual to install protection software on the individual computers if the network itself is not equipped with protection software specifically designed for it. For this reason, CIC is **recommending** the following for networks and networked computers:

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

Implementing these security measures will greatly reduce the risk of technological threats to SPO systems and databases and to iCAMS.



Note: SPOs running networks without network-specific firewall and anti-virus protection software are required to access iCAMS on stand-alone computers equipped with the required protection software as outlined in section 2.1.

SPOs may wish to consider additional protection technology for their networks, such as intrusion detection and content inspection as described below.

Intrusion detection: This 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.

Content inspection: This is like virus detection but in reverse. This software 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.

In addition to network protection software/hardware, we **recommend** that SPOs have:

- A password management system: this is a system managed by a network administrator whereby users are required to install unique log-in passwords and are reminded/required to change them on a regular basis. The network administrator also ensures that repeat and old passwords are eliminated.

As required for stand-alone computers accessing iCAMS, networked computers should also be equipped with password-protected screen savers (an activation period of no more than 15 minutes of non-usage is suggested).

PART III: Physical Security

1. Background

The iCAMS Threat and Risk Assessment reviewed the risk of unauthorized access to information in relation to the physical placement of facilities, including computers, at SPOs. The assessment noted that inadequate physical security could lead to unauthorized access to an iCAMS workstation and/or sensitive information. Furthermore, monitors located in locations 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 on the confidentiality of sensitive information.

2. Requirements

CIC, therefore, requires that the following physical security measures be implemented:

- Monitors of computers, through which iCAMS will be accessed, be faced away from windows or public access areas to prevent unauthorized viewing or access.
- 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 iCAMS.

PART IV: Security Breaches and Violations

E.D.s should instruct all staff, in addition to iCAMS users, to notify them immediately when they become aware of a security violation or breach that may affect the security of client information.

Security breach:

Refers to the unauthorized **disclosure** of client information.

Security violations:

Events that could have led to a security breach but did not.

These events may involve a threat arriving over the Internet, such as a virus or hacker, or unauthorized persons attempting to gain access to client information in iCAMS.

In addition to following their regular security procedures, the E.D. must immediately notify a member of the CIC Contribution Accountability Team (see Appendix A) so that the impact on the iCAMS database can be assessed. The E.D. should also notify the local CIC office administering the contribution agreement. These two offices should be kept informed at regular intervals and of the final outcome whenever an investigation is conducted.

Appendix A

For advice and guidance on applying these requirements please contact:

NATIONAL HEADQUARTERS

Teresa Pires
Program Manager
Integration Branch, Settlement
Citizenship and Immigration Canada
300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1
Tel: (613) 952 – 6321
Fax: (613) 952 – 7416
Email: teresa.pires@cic.gc.ca

Lanielle Caron
Senior Advisor, Policy and Programs
Integration Branch, Settlement
Citizenship and Immigration Canada
300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1
Tel: (613) 952-2561
Fax: (613) 952-7416
Email: lanielle.caron@cic.gc.ca

Catherine Smith
Senior Advisor, Policy and Programs
Integration Branch, Settlement
300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1
Tel: (613) 957 - 8014
Fax: (613) 952-7416
Email: catherine.smith@cic.gc.ca

ATLANTIC

Bruna Caracristi
Program Specialist
Integration Branch, Settlement
Citizenship and Immigration Canada
300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1
Tel: (613) 957-8526
Fax (613) 952-7416
Email: bruna.caracristi@cic.gc.ca

PRAIRIES

Iris Bemister
Program Specialist
Integration Branch, Settlement
c/o CIC Regina
Citizenship and Immigration Canada
1871 Hamilton St.
Regina, SK, S4P 2B9
Tel: (306) 780-5257
Fax: (306) 780-8745
Email: iris.bemister@cic.gc.ca

ONTARIO

John Lu
Program Specialist
Integration Branch, Settlement
C/O OASIS
Citizenship and Immigration Canada
74 Victoria Street, Suite 1001
Toronto, ON M5C 2S1
Tel: (416) 952-8967
Fax: (416) 973-9027
Email: john.lu@cic.gc.ca

Appendix B

iCAMS User Authorization and Reliability Assessment Form <i>(completion optional)</i>			
<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: <input type="checkbox"/> Certificate Number: Date of Issue: Authority:		
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 'iCAMS Security Requirements for Service Provider Organizations', I consider this individual to be reliable for the purposes of accessing iCAMS.			
_____		_____	
Signature		Date	
Name and title of authorized official:	Office Address:	Telephone:	Facsimile:
		()	()

Appendix C

iCAMS User Security Requirements

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

1. Only individuals with an iCAMS username and password are allowed to access iCAMS.
2. 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.
3. Client information in iCAMS is sensitive information and users must keep it confidential at all times in accordance with privacy provisions in the CIC Contribution Agreement.
4. Users are not to leave their computers unattended while logged onto iCAMS.
5. Users must ensure that their computers are equipped with a password-protected screen-saver. An activation period of no more than 15 minutes of non-usage is suggested.
6. Users must face their computer monitors away from windows or public access areas to prevent unauthorized viewing of or access to iCAMS client information.
7. Users are to immediately report all attempts or occurrences involving unauthorized access to iCAMS or iCAMS client information being altered, damaged or stolen to the SPO Executive Director who must immediately report this to a member of the CIC Contribution Accountability Team (see Appendix A).
8. Users who no longer require access to iCAMS must complete the *iCAMS Username and Password Cancellation Form* and indicate that they are aware of their continuing obligation to maintain the confidentiality of the iCAMS information to which they have had access.
9. Users should be aware that CIC monitors and reviews iCAMS activity and that usernames and passwords may be revoked at any time.

Appendix D**iCAMS Username and Password Request/Update Form**

The following information must be provided to request a 'username' and 'password' for a new user of the Immigration-Contribution Accountability Measurement System (iCAMS), to replace a forgotten password or to update user information. Form submission instructions can be found on the last page of this form.

Service Provider Organization (SPO) Contact Information

SPO Name:					
Street Address:					
City:		Province:		Postal Code:	
iCAMS ID Number:					

Executive Director (or Designate) Contact Information

Salutation (Mr., Ms., etc.):		Given Name:		Surname:	
Position Title:					
Telephone Number and Extension:	()	Fax Number:	()		
E-mail Address:					

User Contact Information

Salutation (Mr., Ms., etc.):		Given Name:		Surname:	
Position Title:					
Telephone Number and Extension:	()	Fax Number:	()		
E-mail Address:					

User Access Request: The Executive Director must indicate the program(s) and the corresponding access level (Basic Access = Enter Data, Save, Update, View Reports; Advanced Access = Basic plus Delete, Correct Errors and Administer Data Entry Periods. There should only be one Advanced user per SPO)

iCAMS Programs User Needs Access To (X all that apply):		User Privileges Requested Per Program (X only one per line)			
i. iCAMS-RAP		Basic Access		Advanced Access	
ii. iCAMS-LINC Assessment		Basic Access		Advanced Access	
iii. iCAMS-LINC Training		Basic Access		Advanced Access	
iv. iCAMS-ISAP Aggregate		Basic Access		Advanced Access	
v. iCAMS-ISAP Individual		Basic Access		Advanced Access	
vi. iCAMS-Host Aggregate		Basic Access		Advanced Access	

vii. iCAMS-Host Individual		Basic Access		Advanced Access	
-----------------------------------	--	---------------------	--	------------------------	--

Date User Requires Access (yyyy-mm-dd):	
--	--

The user must supply a **Confidential Question** and **Confidential Answer** below (for example: Confidential Question = My favorite movie is? Confidential Answer = Gone With The Wind). This will allow iCAMS Support to confirm the user's identity.

Confidential Question:	
Confidential Answer:	

USER'S ACKNOWLEDGEMENT:

I, the user, have received an oral or written briefing on the iCAMS User Security Requirements in Appendix C of the "iCAMS Security Requirements for Service Provider Organizations" and I agree to respect them or my access to iCAMS may be removed.

Signature of User:	
Date Signed (yyyy-mm-dd):	

EXECUTIVE DIRECTOR (OR DESIGNATE)'S ACKNOWLEDGEMENT:

I, the Executive Director, have found the user named above to be reliable in accordance with the "iCAMS Security Requirements for Service Provider Organizations" and authorize this application for a username and password with the specified program access and privileges.

Signature of Executive Director:	
Date Signed (yyyy-mm-dd):	

FORM SUBMISSION INSTRUCTIONS:

This form must be mailed with the user's and the Executive Director's original signature. Because the form contains confidential information, it must be double enveloped. Please follow the steps below:

1. Place the completed form in a sealed envelope marked "PROTECTED B" addressed to:

Lanielle Caron
Contribution Accountability Team
Integration Branch, Settlement Division
Citizenship and Immigration Canada
Jean Edmonds Tower North, 300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1

2. Place the above envelope in a **second** envelope with no special marking addressed to the same location.

Receipt of username and password by user: Users will be contacted directly by CIC with their username and password, using the contact information provided on the form.

Appendix E**iCAMS Username and Password Cancellation Form**

The following information must be provided to request a cancellation of a user's 'username' and 'password' in the Immigration-Contribution Accountability Measurement System (iCAMS). A cancellation must be requested when a user is no longer going to use iCAMS. In cases where the user's reliability status has expired or has been revoked or where the user has misused iCAMS, a cancellation must be requested immediately. Form submission instructions can be found on the last page of this form.

Service Provider Organization (SPO) Contact Information

SPO Name:					
Street Address:					
City:		Province:		Postal Code:	
iCAMS Identifier Number:					

Executive Director (or Designate) Contact Information

Salutation (Mr., Ms., etc.):		Given Name:		Surname:	
Position Title:					
Telephone Number and Extension:	()	Fax Number:	()		
E-mail Address:					

User Contact Information

Salutation (Mr., Ms., etc.):		Given Name:		Surname:	
Position Title:					
Telephone Number and Extension:	()	Fax Number:	()		
E-mail Address:					

User Cancellation Request: The Executive Director must indicate the programs that are to be cancelled for the user.

User Access to be Cancelled for these iCAMS Programs (X all that apply):			
iCAMS-RAP		iCAMS-ISAP Aggregate	
iCAMS-LINC Assessment		iCAMS-ISAP Individual	
iCAMS-LINC Training		iCAMS-Host Aggregate	
		iCAMS-Host Individual	

Reason(s) for cancellation – specify the name of the program for which access is cancelled, as appropriate:	
---	--

Date User Account Cancellation to Take Effect (yyyy-mm-dd):	
--	--

USER’S ACKNOWLEDGEMENT:

I, the user, understand that once my iCAMS access is cancelled, I still have a continuing obligation to maintain the confidentiality of the iCAMS client information to which I have had access.

Signature of User:	
Date Signed (yyyy-mm-dd):	

EXECUTIVE DIRECTOR (OR DESIGNATE)’S ACKNOWLEDGEMENT:

I, the Executive Director, authorize the cancellation of iCAMS access, as specified on this form, for the user named above.

Signature of Executive Director:	
Date Signed (yyyy-mm-dd):	

FORM SUBMISSION INSTRUCTIONS:

This form must be mailed with the user’s and Executive Director’s original signature to:

Lanielle Caron
Contribution Accountability Team
Integration Branch, Settlement Division
Citizenship and Immigration Canada
Jean Edmonds Tower North, 300 Slater Street, 5th Floor
Ottawa, Ontario, K1A 1L1

No confirmation of account cancellation will be given unless requested.

--

FEEDBACK FORM (Page 2) <i>iCAMS Security Requirements for Service Provider Organizations</i>
--

--

Comments written by:	
Date:	
Phone number:	
Service Provider Organization:	
City and Province:	
Reviewed by Executive Director:	<input type="radio"/> Yes <input type="radio"/> No (check one)

***Please send comments to the Contribution Accountability Team
at fax number (613) 952-7416 or by e-mail to Catherine.smith@cic.gc.ca. Thank you.**