Employment and Social Development Canada
Emploi et Développement social Canada
Canada

SYSTEMS SUPPORT OPERATIONAL GUIDE (SSOG)

Operational procedures in support of the

PROTECTION OF PERSONAL INFORMATION, SYSTEMS AND SECURITY REQUIREMENTS FOR EXCHANGING INFORMATION AND DATA UNDER THE INDIGENOUS SKILLS AND EMPLOYMENT TRAINING (ISET) PROGRAM FUNDING AGREEMENT

Draft

October 2019

TABLE OF CONTENTS

DRAFT

1.0 GENERAL

1.1 Introduction

The Systems Support Operational Guide (SSOG) is a supporting document to the Indigenous Skills and Employment Training (ISET) Program funding agreement, Part 4 – Service Standards and Data Collection, Articles 26 to 30.

While the agreement reflects the service level standards for use of systems and services administered by Canada, it is important to describe the process details, forms, and protocols required for the Recipients to use. This practice will allow for the updating of procedures when they change, without having to formally amend the funding agreement.

1.2 Amendments

Canada may amend the SSOG from time to time to address operational and security requirements and Canada will provide notice to the Recipient when any change or amendment has been made to the SSOG. Any changes or amendments made to the SSOG shall apply to the ISET Program funding agreement upon the issuance of notice of the changes or amendments by Canada to the Recipient.

1.3 Interpretation

"**Authorized User**" ("**AU**") means employees, contractors and agents of the Recipient, or employees, contractors and agents of a Sub-Agreement, who have been granted access to the Systems and Services Administered by Canada identified in section 4 of this Systems Support Operations Guide.

"Canada's Access Coordinators" means Service Canada's Regional coordinator(s) authorized to submit and manage access requests for the Systems and Services Administered by Canada.

"**Identity Management Credentials** ("**IMC**")" refers to the technological tools, including but not limited to keys, eGrids or software, and any combination of user codes and passwords associated with the required registration and authentication to the Systems and Services Administered by Canada.

"**New user**" refers to an individual that is a proposed Authorized User of the Systems and Services Administered by Canada but has not been yet allocated the required IMC in order to establish a connection to Canada environment;

"**Premiums Paid Eligible (PPE)**" refers to an unemployed person who paid Employment Insurance premiums in at least 5 of the last 10 calendar years that did not

DRAFT

entitle the person to a refund (Note: if the person made less than $2000 income in a year, any EI premiums that they would have paid, would be reimbursed.).

"**Protected B Information**" applies to information or assets that, if compromised, could cause serious injury to an individual, organization or government.

"Recipient" means the recipient organization under the ISET Program funding agreement.

"**Recipient Access Coordinator**" refers to the person who will be responsible for liaising with the Authorized Users and the Canada's Access Coordinator on all matters involving access to Systems and Services Administered by Canada.

"**Reliability Status**" is the successful completion of a reliability check for an individual, which provides the appropriate security clearance for regular access to protected Personal Information through the EIBIS/LMDA Access, Secure ASETS and Secure Data Gateway.

"**Sub-agreement**" means an agreement between the Recipient and an organization other than the Recipient, under which the Recipient further distributes the funds received under this Agreement, and delegates all or part of their responsibilities relating to the delivery of the eligible activities under this Agreement.

"**Systems and Services Administered by Canada**" refers to the systems and services identified in section 4 of the Systems Support Operations Guide.

DRAFT

2.0 ROLES AND RESPONSABILITIES

2.1 Canada is responsible for:

- establishing a secure network connectivity (encrypted) between Canada and the Recipient and between Canada and any Sub-Agreement identified by the Recipient, that allows for access to the Systems and Services Administered by Canada.

2.2 The Recipient is responsible for:

- managing, supporting and maintaining its own technological environment including its network, routers, and workstations;

- ensuring that all Personal Information in the care and control of the Recipient or a Sub-Agreement is protected from misuse and unauthorized access, disclosure, modification, disposal or destruction at all times;

- appointing a Recipient Access Coordinator who will be responsible for liaising with Authorized Users (AUs), employees, agents and contractors of the Recipient and any Sub-Agreement and communicating with Canada's Access Coordinator on all matters involving access to Systems and Services Administered by Canada;

- ensuring that AUs are advised of and abide by their obligations, roles and responsibilities and use Personal Information only for the purposes of sharing under the Agreement, including:

    - ensuring that the identification and authorization information of a new user or an AU collected in support of the application for accessing Systems and Services Administered by Canada is true, valid, accurate and complete, and that the Canada's Access Coordinator is immediately advised if any of that information changes or is no longer valid or accurate;
    - safeguarding all IMC passwords, eGrids, or other security tools and taking all reasonable and necessary measures to prevent the loss, disclosure, modification or unauthorized use of their IMC, and immediately advising the Canada's Access Coordinator with full details when any of the situations set out above occur;
    - ensuring that AUs are accessing the Systems and Services Administered by Canada only by using the IMCs allocated to them and only for the purposes for which they were granted; and

- providing any necessary training and technical support to AUs, including any AUs of a Sub-Agreement.

DRAFT

3.0 SECURITY REQUIREMENTS AND SYSTEMS ACCESS MANAGEMENT

- The Recipient acknowledges and agrees that access to Systems and Services Administered by Canada is governed by Canada's Treasury Board Secretariat's *Policy on Government Security* and its *Policy on Departmental Information Technology Security Management*, as amended from time to time.

- To be granted access to the Systems and Services Administered by Canada listed in section 4 of the SSOG, all new users must undergo a personnel security screening process and obtain a valid Reliability Status.

- Canada has discretion to refuse a personnel security screening of any new user provided by the Recipient.

- Canada will perform the required security screening process for new users and existing AUs who require access to all Systems and Services Administered by Canada and this, for the duration of the present ISET Program funding agreement.

- All requests for the issuance, modification, suspension, or cancellation of the IMC, shall be submitted, processed and managed in accordance with the SSOG and the security policies applicable to the ISET Program funding agreement.

3.1 Reliability Status

Reliability status screening and validation are pre-requisites to being granted access to Canada's systems, and is to be performed by Canada when a new user needs to have access to the Systems and Services Administered by Canada.

Canada's Access Coordinator will provide the Recipient's new user the Personal Screening Consent and Authorization (PSCA) form. The new user will mail the completed form to the Canada's Access Coordinator in a double sealed envelope as required for the secure transport of Protected B information. The Canada's Regional Access Coordinator and Regional Security Office will initiate the screening process.

When the screening process is confirmed successful, the Canada's Access Coordinator will submit the Online Access Request form, completed by the Recipients new user, for processing, to the National Access Coordinator. Once the access request has been completed, the AU will receive an email confirmation from Canada.

If it happens that a Recipient's new user fails to obtain the appropriate reliability status, the Canada's Access Coordinator will immediately inform the Recipient's Access Coordinator that the specific user would not be granted access to Canada's systems.

DRAFT

3.2 Systems Access Management

Recipient Access Coordinator (with confirmed reliability status) will submit a formal request for access by completing the Online Access Request Form as provided by the Canada's Access Coordinator.

The Recipient Access Coordinator will send by e-mail the form to the Canada's Access Coordinator and the Canada's Regional Access Coordinator will follow the internal process for the account creation.

All requests for the AU access modifications should be submitted through the Canada's Access Coordinator. The following list describes the various access management options:

- Add new applications to be granted access to;
- Remove access to specific applications;
- Deactivate / Reactivate user code;
- Password resets;
- Change in the AU's identification information (name, email address etc).

DRAFT

4.0 SYSTEMS AND SERVICES ADMINISTERED BY CANADA

4.1 Systems and Services

Canada will provide the Recipient and any Sub-Agreement identified by the Recipient with access to the following suite of systems and services for the purpose of exchanging Personal Information in accordance with Part 4 of the ISET Program funding agreement:

(a) Employment Insurance Benefits Information System (EIBIS) / Labour Market Development Agreement (LMDA Access);

(b) Secure ASETS;

(c) Data Gateway.

(d) Secure Data Gateway (two-way documents transfer);

(e) ASETS website.

4.2 Computer Configuration Requirements

- Any recent version of a major browser with Secure Sockets Layer (SSL) support.
- All the necessary ports must be opened: 443, 80 (TCP only) outbound on the enterprise firewall and PC firewall (if any).
- Pop up blocker must be configured to allow pop ups from srv100.services.gc.ca.
- The browser used might need to be configured to prevent the use of the same window to launch shortcuts in some cases. This can be done by deactivating the "Reuse windows for launching shortcuts" option from the parameters of your browser (please refer to the instructions related to the browser selected if required). This will prevent the applications from opening on the same page as AppGate which would automatically close the AppGate session and consequently prevent the availability of the applications.
- The Internet connection method is used to support the communication of data between Canada and the Recipient. Internet is a public access network which shares bandwidth with the general public (ie. on the World Wide Web). Although transmission of Protected B personal information is secured (via encryption tools) when obtaining such via Canada's applications, no Protected B information should be exchanged via unencrypted emails between Canada and the Recipient.

DRAFT

4.3 Access Requirements to Systems administered by Canada

The Identity Management Credentials are used by Canada to manage the identification and authentication of the AU's accessing Canada's network infrastructure. Regardless of technology used, the purpose is to allow the systems to uniquely identify the user to Canada's infrastructure. The current, supported technology/solution in use will be detailed further in this document.

4.3.1 Accessing the Secure Canada Network via AppGate (Radius)

The AppGate service will allow for AUs located outside Canada's network to access pre-defined applications located inside the Canada network, by using a supported authentication method (also provided by Canada). This access ensures Protected B information is securely managed between the user's computer and Canada's network.

Who can access AppGate (Radius)?
All AUs requiring access to EIBIS/LMDA Access, Secure ASETS and/or Secure Data Gateway will use AppGate to connect to the Canada network.

How will the user access AppGate (Radius)?
AppGate is accessed using a supported authentication method, such as the eGrid (provided by Canada). These eGrids are used to identify people and resources over networks such as the Internet.

Once AppGate has authenticated the AU on the Canada network, AppGate roles control what the AU has access to. AppGate roles are pre-defined according to the applications required to be accessed by the AU, and are created during the time the AU's access is established.

Troubleshooting
Refer to Section 5.1 Procedure for reporting problems/Incidents for more information.

4.3.2 EIBIS/LMDA Access – Employment Insurance Verification

EIBIS/LMDA Access is a Canada web application that allows AUs to verify Employment Insurance (EI) information and eligibility of a claimant.

The use of this information is two-fold:

1) Verify whether the client has:
    a. an active EI claim in progress, or has had a claim in the last 3-5 years (i.e. former claimant); or
    b. is eligible under the Premiums Paid Eligibility (PPE) criteria; or
    c. is has an active Provincial/Territorial parental benefits / Quebec Parental Insurance Plan (i.e. specials benefits: maternity or parental)

DRAFT

and if so, is entitled to Recipient's EI Part II funded programs and assist Recipient's organizations in determining the nature and level of financial assistance for an active EI claimant eligible for or entitled to assistance under the provincial programs.

2) AUs can use the EIBIS/LMDA Access to submit Section 25 Authorization (S25A) referrals, approving a client to be on training while continuing to receive EI Part I benefits. This is important in order to avoid any disruption in client benefits or pay while participating on Recipients' training program.

Who can access EIBIS/LMDA Access?
All AUs can access EIBIS/LMDA Access after they login in with AppGate, and some of the AUs will also have access to the Section 25 Authorization functionality within the EIBIS/LMDA Access application.

How will the user access the EIBIS/LMDA Access?
AUs will first login to AppGate using their eGrid to be authenticated on the Canada network. Once verified by AppGate, the user will be taken directly to the Canada application they have been granted access to, as determined by the AppGate role associated to their access credentials. AUs having access to more than one Canada application will be directed to a screen where they can select the application they wish to access at that time.

AUs will be issued a unique username and a password. The Recipients Access Coordinators will be responsible for notifying their Canada's Access Coordinator of any changes in capability requirements, deletions, additions, etc. of those user accounts, according to procedures in Section 3.2 of this document.

Troubleshooting

The EIBIS/LMDA Access application contains a Help section which provides basic troubleshooting tips should users experience errors while navigating the application.

For all other issue, refer to the Procedure for reporting problems/Incidents within Section 5.1.

4.4.3 Secure ASETS

Secure ASETS is a secure Canada website where the AUs can access the Social Insurance Number (SIN) level data to help reconcile their organization results against departmental results. The SIN level data provided on the website allows AUs to identify exactly which client files did not meet the Canada business calculation rules (one result per year, per client, per program; 24-week rule and 12-week / 25% rule).

DRAFT

In identifying which client results were rejected for not meeting a particular business rule, only the SIN and the Action Plan Start Date are provided. With this information, the AUs can go into their organization's case management system, identify the client record, review the information and make any modification, if required.

Who can access the Secure ASETS?
All AUs can access Secure ASETS after they login in with AppGate.

How will the user access the Secure ASETS?
The AU will be issued a unique user code and password to access the Secure ASETS website. The AU also needs to have a username and password for the ASETS Members website, as Secure ASETS uses the information from this website to identify which results the AU can access.

AUs will first login to AppGate using their eGrid to be authenticated on the Canada network. Once verified by AppGate, the user will be taken directly to the Canada application they have been granted access to, as determined by the AppGate role associated to their access credentials. AUs having access to more than one Canada application will be directed to a screen where they can select the application they wish to access at that time.

The Recipients Access Coordinators will be responsible for notifying their Canada's Access Coordinator of any changes in capability requirements, deletions, additions, etc. of those user accounts, according to procedures in Section 3.2 of this document.

Troubleshooting
Refer to Section 5.1 Procedure for reporting problems/Incidents for more information.

4.4.4 Data Gateway

The Data Gateway is a web-based file transfer service used to upload Recipients' clients information via a predetermined XML file to Canada. Note: the Data Gateway does not show the results of the Recipient.

Who can access the Data Gateway?
All AUs requiring access as determined by the Recipient's Access Coordinator, and confirmed by one of Canada's Access Coordinator.

How will the user access the Data Gateway?
AU's require a unique user name and password to access their organization profile on the Data Gateway in order to upload their client's information in an XML format. No login via AppGate is required to access the Data Gateway.

Troubleshooting
Refer to Section 5.1 Procedure for reporting problems/Incidents for more information.

DRAFT

4.4.5 Secure Data Gateway

The Secure Data Gateway is a secured exchange web site, which allows the Recipient to exchange Protected B information (upload-download) with Service Canada.

Who can access the Secure Data Gateway?
Only the AUs requiring access as determined by the Recipient's Access Coordinator will have access to transfer the EI documentations to the Regional Service Canada Representatives.

How will the user access the Secure Data Gateway?
Login via AppGate is required to access the Secure Data Gateway.

Troubleshooting
Refer to Section 5.1 Procedure for reporting problems/Incidents for more information.

4.4.6 ASETS Website

Definition
The ASETS Website allows the Recipients and the AUs to consult documents related to the Indigenous programs as well as to view the aggregate reports on the results of their organization.

Who can access the ASETS Website?
All AUs requiring access as determined by the Recipient's Access Coordinator can have access to the ASETS Website.

How will the user access the ASETS Website?
A unique user name and a password will be created for each user that will give access to their organization profile and results on the ASETS Website. No login via AppGate is required to access the ASETS Website, as there is no personal information on this website.

Troubleshooting
Refer to Section 5.1 Procedure for reporting problems/Incidents for more information.

DRAFT

5.0 PROBLEM MANAGEMENT PROCEDURES

5.1 Procedure for reporting problems/Incidents

The AU contacts their Recipient Access Coordinator to report the issue and provide as much detail as possible about the issue.

The Recipient Access Coordinator determines if the problem is internal to the Recipient's network or if it is a Canada systems problem.

If the problem is determined to be internal to the Recipient's network, the Recipient Access Coordinator will notify the technical unit in charge to remedy the problem.

If the problem is identified as originating from Systems and Services administered by Canada, the Recipient Access Coordinator will contact the Canada's Access Coordinator and report the issue, providing as much detail as possible to help resolve the problem.

The Canada's Access Coordinator will determine if the issue is business related or IT/systems related. In the case of system's related issues, the appropriate Canada's Access Coordinator will report the incident to the National Access Coordinator while the business related issues will be dealt with within the Service Canada regional business unit.

DRAFT

6.0 CHANGE MANAGEMENT AND NOTIFICATION PROCESS

6.1 Change Management

Changes to Recipients' technological infrastructure are determined in advance during each organization's planning cycle. As a result, these changes could affect the organization's infrastructure (e.g. networks, software) and it is their responsibility to ensure these changes will not impact on their access to the systems administered by Canada. Therefore, the Recipients are invited to exchange such information as soon as each organization's planning cycle is determined. The Recipient Access Coordinator will share planned changes with the Canada's Access Coordinator to identify potential areas of respective impacts and discuss accordingly.

6.2 Notification to the Recipients and Authorized Users

At any time where a system administered by Canada will not be available to the AUs, a notification will be distributed to the Recipients Access Coordinator and the AUs. Notifications will be sent via email or display on the affected system and will include the changes that are being applied, and the scheduled date and time of the unavailability.

DRAFT