



**GUIDE**

---

**Market Manual 1: Market Entry,  
Maintenance & Exit**

**Part 1.3: Identity  
Management Operations  
Guide**

---

**Issue 28.0**

This guide describes the processes for *Market Participants* and the *IESO* to register for, initialize, change, and revoke User Accounts and request system access privileges required for access to *IESO*-secure Web servers.

## Disclaimer

The posting of documents on this Web site is done for the convenience of *market participants* and other interested visitors to the *IESO* Web site. Please be advised that, while the *IESO* attempts to have all posted documents conform to the original, changes can result from the original, including changes resulting from the programs used to format the documents for posting on the Web site as well as from the programs used by the viewer to download and read the documents. The *IESO* makes no representation or warranty, express or implied that the documents on this Web site are exact reproductions of the original documents listed. In addition, the documents and information posted on this Web site are subject to change. The *IESO* may revise, withdraw or make final these materials at any time at its sole discretion without further notice. It is solely your responsibility to ensure that you are using up-to-date documents and information.

This *market manual* may contain a summary of a particular *market rule*. Where provided, the summary has been used because of the length of the *market rule* itself. The reader should be aware however; that where a *market rule* is applicable, the obligation that needs to be met is as stated in the “*market rules*”. To the extent of any discrepancy or inconsistency between the provisions of a particular *market rule* and the summary, the provision of the *market rule* shall govern.

<b>Document ID</b>	IMP_GDE_0088
<b>Document Name</b>	Part 1.3: Identity Management Operations Guide
<b>Issue</b>	Issue 28.0
<b>Reason for Issue</b>	Issue released for Baseline 46.0.
<b>Effective Date</b>	September 15, 2021

## Document Change History

Issue	Reason for Issue	Date
For change history prior to Issue 17.0, see Issue 21.0		
17.0	Revised for Verizon CA Renewal May 2010 in advance of Baseline 23.1	March 26, 2010
18.0	Revised for removal of requirements for PKI certificate login for Portal Transmission Rights Auction access	June 12, 2010
19.0	Revised for removal of all requirements for PKI certificates	September 12, 2012
20.0	Revised for addition of stronger authentication components, methods and content	March 6, 2013
21.0	Revised in advance of Baseline 31.0 for the change to the IESO's online registration business process management tool. As a replacement for the 1276 form.	February 14, 2014
22.0	Revised for Baseline 36.1 for changes within Online IESO for registration business processes, addition of new applications and replacement of market facing applications for Energy Market, Reliability Compliance, Outage Management and other web based functions.	December 7, 2016
23.0	Revised for Baseline 38.1 for changes to reflect the decommissioning of the Market Information Management <i>IESO</i> Development Kit (MIM IDK).	December 6, 2017
24.0	Revised for Baseline 41.0 regarding the removal of the need for a Java Runtime Environment (JRE) and java policy file for multiple file upload capability for the Portal.	March 6, 2019
25.0	Revised in advance of Baseline 42.1 to reflect changes as a result of the transition of the <i>demand response auction</i> to the <i>transitional capacity auction</i>	October 15, 2019
26.0	Updated to meet accessibility requirements pursuant to the <i>Accessibility for Ontarians with Disabilities Act</i>	November 3, 2020
27.0	Issue released in advance of Baseline 45.0. Updated to include electricity storage participation.	February 26, 2021
28.0	Issue released for Baseline 46.0. Updated for changes to authentication system for all Market Facing systems including the Reports site and decommissioning of the IESO Portal and addition of the Okta based IESO Gateway system.	September 15, 2021

## Related Documents

Document ID	Document Title
N/A	IESO Gateway User Guide

# Table of Contents

---

<b>1. Introduction .....</b>	<b>3</b>
1.1 Purpose .....	3
1.2 Scope .....	4
1.3 Who Should Use This Document .....	4
1.4 Overview .....	5
1.4.1 Provisioning, Identity Management, the <i>IESO</i> and the <i>Participant</i> .....	5
1.4.2 User Account Identity Credentials .....	5
1.5 Assumptions and Limitations .....	7
1.6 Conventions.....	7
1.7 Document Organization .....	7
1.8 Contact Information .....	7
<b>2. Roles and Responsibilities of Identity Management Entities .....</b>	<b>8</b>
<b>3. Identity Trust Operational Model .....</b>	<b>10</b>
3.1 IESO Trust Model .....	10
3.2 Identity Proofing.....	11
3.3 Rights Administrator Model.....	11
<b>4. Identity Management Procedural Work Flows .....</b>	<b>13</b>
4.1 Participant User Account Application Scenario .....	14
4.2 Participant User Account Change Scenario 1 .....	15
4.3 Participant User Account Change Scenario 2 .....	16
4.4 Participant User Account De-provisioning / Deactivation Scenario.....	17
4.5 Participant User Account Recovery Scenario 1 .....	18
4.6 Participant User Account Recovery Scenario 2.....	19
4.7 Participant Rights Administrator Enrolment Scenario.....	20
4.8 Participant Rights Administrator User Account Change Scenario 1 .....	21
4.9 Participant Rights Administrator User Account Change Scenario 2 .....	22
4.10 Participant Rights Administrator Role Termination Scenario .....	23
4.11 Subscriber User Account Initialization / Password Reset .....	24
4.12 Periodic Update of Subscriber User Account Password.....	25
<b>5. Participant Primary Contact Operational Guidelines .....</b>	<b>26</b>
5.1 Primary Contact Definition .....	26
5.2 IESO Trust Model and Identity Credential Proofing.....	26
5.2.1 Participant Rights Administrator .....	26
5.3 Appointing a Rights Administrator.....	26

5.4	Process to Register a Rights Administrator and Request an Account and System Access .....	27
5.5	Requesting a Person’s Rights Administrator Role Termination .....	27
5.5.1	Circumstances for Deactivation of IESO Systems Access and User Account.....	27
5.6	Steps for Registering a Rights Administrator for Registration System Access and a User Account.....	27
<b>6.</b>	<b>Participant Rights Administrator Operational Guidelines .....</b>	<b>28</b>
6.1	Rights Administrator Definition.....	28
6.2	Instructions for Using the IESO Registration System .....	28
6.3	IESO Trust Model and Guidelines for Proofing Credential Subscribers.....	28
6.3.1	When should the Identity of a Credential Subscriber Be Proofed .....	29
6.3.2	Process to Validate the Identity of the Credential Subscriber .....	29
6.4	Guidelines for Form Storage, Protection, and Archival.....	29
6.5	IESO Customer Relations Communications.....	30
6.6	Guidelines for Distributing and Using Identity Credential Activation Data.....	30
6.6.1	IESO Personal User Account Credentials .....	31
6.6.2	User Account Password Reset.....	32
6.6.3	Delivery of Password Reset Email .....	32
6.6.4	Delivery of Temporary password from Customer Relations.....	33
6.7	Person ID Number .....	33
6.8	Basic Trouble Shooting.....	33
<b>7.</b>	<b>Credential Subscriber Operational Guidelines .....</b>	<b>34</b>
7.1	Introduction.....	34
7.2	IESO Trust Model and Identity Credential Proofing.....	34
7.2.1	Participant Rights Administrator .....	35
7.3	Protection of Identity Credential Activation Data .....	35
7.4	Person ID Number .....	35
7.5	Password Creation Guidelines.....	35
7.6	Applying for an IESO Account .....	36
7.7	IESO Systems Access Requests .....	36
7.8	IESO Account Deactivation.....	36
7.8.1	Account Deactivation .....	36
7.9	IESO Account Change.....	37
7.10	Account Recovery.....	37
<b>8.</b>	<b>Use of the Online IESO Registration System.....</b>	<b>38</b>
8.1	Introduction.....	38
8.1.1	Login to the Online IESO System.....	39
8.1.2	Online IESO - Registration Application Actions .....	41
8.1.3	Online IESO Registration System Grant/Revoke Access .....	55

8.1.4	Registration System Manage Contact Information.....	71
<b>9.</b>	<b>Use of Account Provisioning Tools.....</b>	<b>74</b>
9.1	Use of the Password Change & Reset Functions.....	74
9.1.1	User Account Initialization .....	75
9.1.2	Self-Service Password Reset.....	79
9.1.3	Temporary Password Change by IESO Customer Relations.....	81
9.1.4	User Security Profile Options .....	85
9.1.5	Troubleshooting .....	89
<b>10.</b>	<b>Browser Use .....</b>	<b>90</b>
10.1	Browser Versions.....	90
<b>11.</b>	<b>MIM Application Web Services.....</b>	<b>91</b>
11.1	Introduction.....	91
11.2	Downloading the MIM Web Services Files.....	91
<b>Appendix A:</b>	<b>Account Management Procedural Steps .....</b>	<b>A-1</b>
A.1	Participant Account Application Scenario.....	A-1
A.2	Participant Account Change Scenario 1.....	A-2
A.3	Participant User Account Change Scenario 2 .....	A-5
A.4	Participant User Account De-provisioning / Deactivation Scenario.....	A-6
A.5	Participant User Account Recovery Scenario 1 .....	A-8
A.6	Participant User Account Recovery Scenario 2.....	A-10
A.7	Participant Rights Administrator Enrolment Scenario.....	A-12
A.8	Participant Rights Administrator User Account Change Scenario 1 .....	A-14
A.9	Participant Rights Administrator User Account Change Scenario 2 .....	A-16
A.10	Participant Rights Administrator Role Termination Scenario .....	A-1
A.11	Credential Subscriber User Account Initialization / Password Reset .....	A-3
A.12	Periodic Update of Subscriber User Account Password (where required) Scenario .....	A-5
A.13	Description of Changes .....	A-7
A.13.1	Credential Subscriber Information .....	A-7
A.13.2	Rights Administrator Information .....	A-8
<b>Appendix B:</b>	<b>Glossary of Terms .....</b>	<b>B-9</b>
<b>Appendix C:</b>	<b>List of Participations .....</b>	<b>C-1</b>
<b>References</b>	<b>.....</b>	<b>1</b>

# List of Figures

---

Figure 4-1: Participant User Account Application Scenario.....	14
Figure 4-2: Participant User Account Change Scenario 1 .....	15
Figure 4-3: Participant User Account Change Scenario 2 .....	16
Figure 4-4: Participant User Account Deprovisioning / Deactivation Scenario .....	17
Figure 4-5: Participant User Account Recovery Scenario 1 .....	18
Figure 4-6: Participant User Account Recovery Scenario 2 .....	19
Figure 4-7: Participant Rights Administrator Enrolment Scenario .....	20
Figure 4-8: Participant Rights Administrator Account Change Scenario 1 .....	21
Figure 4-9: Participant Rights Administrator Account Change Scenario 2 .....	22
Figure 4-10: Participant Rights Administrator Role Termination Scenario.....	23
Figure 4-11: Subscriber User Account Initialization /Password Reset.....	24
Figure 4-12: Periodic Renewal of User Account Password .....	25
Figure 8-1: IESO Gateway Login Page with Legal Disclaimer .....	39
Figure 8-2: Gateway System Landing Page Example .....	40
Figure 8-3: Online IESO Applicant Representative - Actions Page.....	41
Figure 8-4: Online IESO Applicant Representative – Select Participation Type Page .....	41
Figure 8-5: Online IESO Applicant Representative – Select Participation Type Option.....	42
Figure 8-6: Online IESO Applicant Representative – Market Participation Type.....	42
Figure 8-7: Online IESO Applicant Representative – Market Participation Choices .....	42
Figure 8-8: Online IESO Applicant Representative – Choosing Capacity Auction Market Participation.....	43
Figure 8-9: Online IESO Applicant Representative – Participation Required Tasks.....	43
Figure 8-10: Online IESO Applicant Representative Update Organization Request Type .....	44
Figure 8-11: Online IESO Applicant Representative Update Contact Role(s) Update Type.....	44
Figure 8-12: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search .....	45
Figure 8-13: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search Results .....	46
Figure 8-14: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search Results 2 .....	46
Figure 8-15: Online IESO Applicant Representative Update Contact Role(s) Selection for Selected Person .....	47
Figure 8-16: Online IESO Applicant Representative Update Contact Role(s) Added Person.....	48
Figure 8-17: Online IESO Applicant Representative Update Contact Role(s), Confirmation .....	49
Figure 8-18: Online IESO Applicant Representative Update Contact Role(s), Final Confirmation .....	49
Figure 8-19: Online IESO Applicant Representative Update Contact Role(s) Select Contact Role List.....	50
Figure 8-20: Online IESO Applicant Representative Update Contact Role(s) – Existing Contacts.....	51
Figure 8-21: Online IESO Applicant Representative Update Contact Role(s) – Existing plus New Contacts .....	52
Figure 8-22: Online IESO Applicant Representative Update Contact Role(s) – Primary Confirmation .....	53
Figure 8-23: Online IESO Registration System Rights Administrator Actions Page .....	54
Figure 8-24: Online IESO Registration System Normal Contact Actions Page .....	54
Figure 8-25: Choose an Organization Page.....	55
Figure 8-26: Select System Access Request Type Page .....	56
Figure 8-27: Select Account Type Page - Grant .....	56
Figure 8-28: Search for a Registered Person Page - Grant .....	57
Figure 8-29: Select a Registered Person Page - Grant .....	58
Figure 8-30: Register a New Person Page - Grant .....	59
Figure 8-31: Confirm New Person Registration Page - Grant .....	60
Figure 8-32: Select Access Roles to be Granted Page.....	61
Figure 8-33: Confirm Access Role(s) to be Granted Page .....	62
Figure 8-34: Select Access Roles to be Revoked Page .....	63
Figure 8-35: Confirm Access Role(s) to be Revoked Page .....	64
Figure 8-36: Select Machine Account Page - Grant.....	65

Figure 8-37: Select Machine Account Page - Revoke .....	66
Figure 8-38: Confirm Existing Machine Account Page - Grant .....	67
Figure 8-39: Create Machine Account for Access Role Grant Page .....	68
Figure 8-40: Select Access Role(s) to be Granted – Machine Account Page .....	69
Figure 8-41 Confirm Access Role(s) to be Granted – Machine Account Page .....	70
Figure 8-42 Choose an Action Page .....	71
Figure 8-43 Update Person Information Page .....	72
Figure 8-44 Confirm Person Information Page .....	72
Figure 9-1: Gateway Activation Email – Activate Account Link .....	75
Figure 9-2: Gateway Activation Email – Activate Account Page.....	76
Figure 9-3: Gateway Multifactor Authentication Options Setup.....	76
Figure 9-4: SMS Message Country and Phone Number Setup .....	77
Figure 9-5: SMS Code Receipt and Entry Verification.....	77
Figure 9-6: Security Question and Answer Input.....	78
Figure 9-7: Login Page – Need Help Signing in Link.....	79
Figure 9-8: Login Page – Forgot Password Link .....	79
Figure 9-9: Reset Password – Reset Method Choice .....	80
Figure 9-10: Reset Password – Reset Via Email .....	80
Figure 9-11: Customer Relations Reset Password – Reset Via Email .....	82
Figure 9-12: Customer Relations Reset Password via Email – Password Reset Page .....	83
Figure 9-13: Login Page Using Temporary Password .....	84
Figure 9-14: Password Reset – Entering Old Temporary Password .....	84
Figure 9-15: Password Reset – Entering New Password .....	85
Figure 9-16: IESO Gateway – User Dashboard Settings.....	85
Figure 11-1: Market Information Management Application Interface (Web Services) Download .....	91

# List of Tables

---

Table 2-1: Identity Management Roles and Responsibilities .....	8
Table 4-1: Legend for Work Flow Diagrams .....	13
Table A-1: Participant User Account Application Scenario Task Details.....	A-1
Table A-2: Account Change Scenario 1 Task Details.....	A-2
Table A-3: Participant User Account Change Scenario 2 Task Details .....	A-5
Table A-4: Participant User Account De-Provisioning / Deactivation Scenario Task Details .....	A-6
Table A-5: Participant User Account Recovery Scenario 1 Task Details .....	A-8
Table A-6: Account Recovery Scenario 2 Task Details .....	A-10
Table A-7: Rights Administrator Enrolment Scenario Task Details.....	A-12
Table A-8: Rights Administrator Change Scenario 1 Task Details.....	A-14
Table A-9: Participant Rights Administrator Account Change Scenario 2 Task Details .....	A-16
Table A-10: Participant Rights Administrator Role Termination Scenario Task Details .....	A-1
Table A-11: Credential Subscriber, Account Initialization Task Details .....	A-3
Table A-12: Update of Account Passwords .....	A-5



# Table of Changes

<b>Reference (Section and Paragraph)</b>	<b>Description of Change</b>
Section 1	Added references and content to other Market Facing applications such as Transmissions Rights Auction, Dispatch Services and IESO Workspaces with updated context for such. Removed all references to IESO Portal and added content for IESO Gateway.
Section 2	Removed references to ITOPS Customer Support and replaced with IESO Access Management
Section 3	Added content regarding automated account provisioning. Added reference to Okta as the IESO's authentication system provider.  Updated content and context regarding Rights Administrator model and added reference to email based IESO workspace accounts.
Section 4	Updated all process workflow diagrams to remove references to ITOPS Customer Support and added content and context for the IESO Gateway system and automated account provisioning. Corrected some process diagrams for other content.
Section 6	Updated content to reference the IESO Gateway system, IESO Workspaces and other market facing applications. Added reference to the IESO Gateway User Guide. Removed all references to the IESO Portal.  Updated content and context regarding User Accounts and Password Reset processes for such
Section 7	Updated to include other market facing applications and the IESO Gateway.  Updated password creation guidelines content.  Included reference to automated account provisioning for account creation, access requests, account deactivation, account changes and account recovery.
Section 8	Updated content to remove all references to IESO Portal, ITOPS Customer Support and added content for IESO Gateway. Added content on automated account provisioning with IESO Gateway.
Section 9	Updated all content to remove all references to IESO Portal, ITOPS Customer Support and added content for IESO Gateway. Added content on automated account provisioning with IESO Gateway.
Section 10	Removed content on specific browser versions. Reference left only to IESO supported client platform page.
Section 11	Removed reference to Internet Explorer and added reference to Edge and Chrome browsers.
Appendix A	Updated all tables and content to match updated process flow diagrams in section 4.
Appendix B	Added reference to IESO Gateway system to Glossary.

# 1. Introduction

---

## 1.1 Purpose

The “Identity Management Operations Guide” describes the various processes for user provisioning and identity management that are employed to manage users regarding registration, authentication, authorization of access permissions to the various market systems, self-service, as well as disabling and termination of user accounts. This guide provides information on identity management processes for the market systems.

Included is the definition of what provisioning and identity management are, the detailed *participant* guidelines for dealing with provisioning and Identity Management, and the guidelines for *participant* management of user accounts and identity credentials throughout their lifecycle.

Each individual within an organization participating in the *IESO-administered markets* must possess valid and appropriate user identity credentials such as a User Account / password for proper authentication and access to *IESO-secure Web servers* and or *Web Services*. Activities for which access to *IESO-secure Web servers* or *Web Services* is required include, but are not limited to, the following:

- Accessing the Energy Market Interface system for Entering *bids/offers*
- Accessing the Transmission Rights Auction system;
- Accessing IESO Workspaces (formerly Watchdox) and which now hosts all the former Collaboration communities such as the SOE LDC Extranet and MACD communities. Portal Collaboration is being decommissioned as a result.
- Accessing the Confidential and Public Reports system (IESO Reports Site);
- Accessing the Meter Trouble Reporting (MTR) via Online IESO;
- Accessing the Notice of Disagreement (NOD) via Online IESO;
- Accessing the Reliability Compliance System via Online IESO;
- Accessing the Prudential system via IESO Online;
- Accessing the Capacity Auction via Online IESO;
- Accessing the Energy Limited Forecast system via Online IESO;
- Accessing the CROW Outage Management system;
- Accessing the Dispatch Services system;
- Accessing the Registration system via Online IESO:
  - By individual users for managing their own person information and accessing market functionality;
  - By organizations’ Rights Administrators and Applicant Representatives to register for, initialize and provision accounts, change, and revoke user accounts and register contact roles and request system access privileges required for access to *IESO-secure Web servers* for people within their organizations.

- By organizations' Applicant Representatives to register Facilities and Equipment associated to their organizations.

*IESO* web servers, systems, and business processes shall in most cases require the use of appropriate user identity credentials (e.g. UserID based User Account / Password) for authentication and authorization purposes. *IESO* Workspaces will require a separate email based account.

All web based applications, excluding the *IESO* Reports site and any application web services shall be accessible by navigating to the new *IESO* Gateway system at: <https://gateway.ieso.ca>. Sandbox environment applications are accessible at: <https://gateway-sbx.ieso.ca>

An organization must have applied for authorization to participate in the *IESO-administered markets* or applied for *Metering Service Provider* (MSP) registration before its employees or representatives can apply for their user account / identity credentials. See “Market Manual 1: Market Entry, Maintenance & Exit, Part 1.1: Participant Authorization, Maintenance & Exit, or the Market Manual 3: Metering, Part 3.1: Metering Service Provider Registration, Revocation, and De-registration”.

## 1.2 Scope

This document will help to guide the actions taken by the *participants* regarding user provisioning and identity credentials, such as user registration and other related processes including those for User Account / password for users under their span of control. The document provides the *participant* with the *IESO* approved Identity Proofing options, different provisioning and identity management process scenarios, as well as the Operational Guidelines for the Primary Contact and the Rights Administrator. This document explains the following:

- What user provisioning and identity management is and why it is necessary;
- What user accounts / credentials are and what forms they can or may take;
- The standards employed for user accounts / credentials;
- Roles and Responsibilities of identity management entities;
- *IESO* approved Identity Proofing Model;
- How provisioning for user accounts / credentials and system access control works within identity management regarding:
  - What delegated user administration is and how it is used;
  - How to make authorized requests for a user account / credentials;
  - How to initialize various user credentials;
  - How to request changes affecting a user account / credentials;
  - How to reset and or change a User Account's password and answers to security questions where applicable;
  - The conditions under which a user credential may be revoked;
  - How to apply for a deactivation or termination of user account / credentials;
  - How to obtain and learn about the MIM Web Services package.

## 1.3 Who Should Use This Document

This document is intended for *participant* individuals, i.e. Primary Contacts and Rights Administrators who will be involved in the provisioning of users and identity management for the

management of user accounts / credentials. This document was designed so that the Primary Contact Operational Guidelines; the Rights Administrator Operational Guidelines; the Individual Subscriber Operational Guidelines, could be separated out and delivered to the appropriate individuals fulfilling those roles.

## 1.4 Overview

Information security is a priority for organizations that conduct communications and business transactions via the Internet. Identity Management, including user provisioning, is a set of processes used for managing authentication, authorization and access to information systems. Identity management means ensuring that only the intended users have the required credentials, access and the correct level of privileges to secured information. Identity management deals with credentials such as User Account / Password and security questions and information.

Provisioning is the set of identity management processes and tools used for actually defining and securing proper access credentials and privileges to users. This includes the use of tools and activation codes, information or temporary passwords supplied during the registration and user account provisioning process to provide for online initialization of the credentials as well as password changes, password reset, credential recovery, credential renewal etc.

To ensure security and confidentiality, identity credential rules around things like password construction and use need to be enforced. This means strong passwords (i.e. eight characters or more, upper and lower case plus numeric and special characters). Regular password changes may also be required but where not, are recommended, typically every 90 days and reuse of old passwords is prohibited.

### 1.4.1 Provisioning, Identity Management, the *IESO* and the *Participant*

The *IESO* identity management trust model provides for the *participant* organization to assume most of the responsibilities of identity management in regards to the proofing of individuals and handling of end user credentials. Please reference the [“Identity Trust Operational Model”](#) in Section 3 to gain a better understanding of the *IESO* approved identity proofing model.

### 1.4.2 User Account Identity Credentials

The *IESO* employs User Accounts (in combination with passwords). User Accounts issued with the identity management system shall adhere to *IESO* global naming conventions and be enforced / validated during provisioning. Unique user identifiers shall remain permanently tied to an individual or machine/application account and to no other. This reduces the risk that any new *participant*' employees, service providers etc. will receive inadvertent erroneous access to confidential market systems, resources or information. Account rationalization to all market systems at the *IESO* has been essentially realized. Only one credential set will be issued to any given person where possible for all market facing systems except where noted. This shall mean that at most, a user will receive one personal User Account where feasible. The exceptions are the new *IESO* Workspaces application (replaces Watchdox and Portal Collaboration) which requires a separate email based account and for users who represent more than one participant for the Transmission Rights auction where they will need a separate UserID based account for each participant they represent.

The *market rules* governing the *IESO* and *participants* require that the *IESO* provide access control for confidentiality of information over electronic communications. The use of identity management

processes, including available user provisioning tools, to supply User Accounts allows the *IESO* to fulfill the appropriate *market rules* governing confidentiality. Properly managed UserID and email based accounts can be used to establish authentication, authorization, and integrity.

Before registering for and provisioning any *IESO* identity credential, *participant* individuals should be positively identified by their organization through a secure method of authentication, as an individual or application user is bound to the credential appropriately issued to them. Each user account / credential when issued will be registered to an individual person and as such these people are known as 'Credential Subscribers'. *Participant* Credential Subscribers may be one of the following:

- a. Authorized Representatives
- b. Primary Contacts
- c. Rights Administrators
- d. Individual Subscriber, (For a User Account, access up to and including transaction level systems and information by a person) for access to IESO market facing systems as one or more of the contact roles listed in Appendix B.
- e. Application Subscriber (machine account; access up to and including transaction level systems and information by a computer application)

Each Authorized Representative, Primary Contact and Rights Administrator shall be issued a User Account for access to the Registration system and for other IESO transaction system level access where applicable by the person's roles.

For the typical Individual Subscriber (and where required an Application Subscriber) a User Account credential will be automatically issued to the target user upon authorized registration for access to the appropriate systems and applications. An account activation link via email shall be supplied in conjunction with the User Account credential for a User account for the Reports site, Energy Market Interface, Outage Management system, Dispatch Services system, Transmission Rights Auction, Prudential Manager, IESO Workspaces, Online IESO system for, Registration and any other application purposes or where applicable Web Services.

The password needs to be setup by the end user through activating their account by initially navigating to the IESO Gateway link as indicated in an email sent to the user during automated account provisioning. The new *IESO Gateway User Guide* details the process for doing so. The activation link will expire automatically after a fixed period of time (90 days) during which time the end user can activate their account via the IESO Gateway link. After the link expires, a request to IESO Customer Relations will be required to issue a temporary password for the account.

Upon initial navigation to the IESO Gateway link, the user shall be required to setup their password using the documented online web provisioning process and to select a multifactor authentication method as well as choose a security question and answer. The multifactor authentication (MFA) process may be presented to the user on each login to the IESO Gateway to provide confidence that user is the one registered and that the authentic IESO system is being connected and logged in to. The MFA method chosen by the user shall be usable by the IESO Gateway to confirm the user's identity as required under circumstances where that identity is suspect. This would include logging in from different workstations, odd times of day compared to the user's normal practices etc. so the user should not be surprised to see the MFA prompt presented during login even when the correct password has been entered. The security question and answer will also be used to permit the users to reset their own passwords if forgotten during login. The IESO Gateway's password setup procedure shall ensure that the password the user chooses meets *IESO* global security policies and standards. Any replacement passwords if and when required shall meet the same security policies and standards.

The user shall after login to the Gateway, be able to change their password as well as documented in the IESO Gateway User Guide.

A person's Gateway user account is common to the, Online IESO system, Energy Market Interface, CROW Outage Management System (OCSS), TRA Auction, Prudential Manager, Dispatch Service and Reports site where that user has access to any of those systems. This means the same account UserID and enduring password is used for access to each system. A separate email based account is required for access to the IESO Workspaces system which is also accessed via the IESO Gateway using that separate email based account.

Individual persons and *participant* programmatic applications (represented by a custodian) accessing the appropriate market systems will use these types of credentials.

## 1.5 Assumptions and Limitations

None.

## 1.6 Conventions

The market manual standard conventions are as defined in the 'Market Manual Overview' document.

## 1.7 Document Organization

1. Introduction
2. Roles and Responsibilities of Identity Management Entities
3. Identity Proofing Operational Models
4. Identity Management Procedural Work Flows
5. Primary Contact Operational Guidelines
6. Rights Administrator Operational Guidelines
7. Credential Subscriber Operational Guidelines
8. Identity Management Procedural Steps (Appendix A)

## 1.8 Contact Information

If the *participant* wishes to contact the *IESO*, the *participant* can contact the *IESO* Customer Relations via email at [customer.relations@IESO.ca](mailto:customer.relations@IESO.ca) or via telephone, mail or courier to the numbers and addresses given on the *IESO*'s Web site ([www.IESO.ca](http://www.IESO.ca)) or click on 'Have a question?' to go to the 'Contacting the *IESO*' page. If *IESO* Customer Relations is not available, telephone messages or emails may be left in relevant voice or electronic *IESO* mail boxes, which will be answered as soon as possible by Customer Relations Staff.

– End of Section –

## 2. Roles and Responsibilities of Identity Management Entities

**Table 2-1: Identity Management Roles and Responsibilities**

Title	Description	
<b>IESO</b>		
<i>IESO</i> Access Management	<i>IESO</i> Access Management is responsible for managing credential issuance, user name changes and credential deactivation requests where required using appropriate tools and procedures, (i.e. for processing requests to <i>IESO</i> systems administrators).	
<i>IESO</i> Customer Relations	<i>IESO</i> Customer Relations is responsible for managing credential recovery requests using appropriate tools and procedures.	
<b>Participant</b>		
Participant Organization	An organizational entity defined for use of an <i>IESO</i> service. Its employees, who possess <i>IESO</i> User Accounts, are referred to as Participant Individual Subscribers or Participant Application Subscribers. Participant roles available for market activities are listed in Appendix C.	
Authorized Representative	A senior officer at a Participant Organization who can authorize one or more officers (i.e., a high-level employee) of the Participant Organization to perform the responsibilities of a Primary Contact regarding Rights Administrator registration for Identity Management.	
Primary Contact	Any officer of a Participant Organization who is authorized by an Authorized Representative to register Rights Administrators for identity management services on behalf of the Participant Organization. The Primary Contact designates and delegates the role of the Rights Administrator via the Online <i>IESO</i> Registration system This shall be done during initial registration or any time after, if not already done and for any subsequent changes to Rights Administrators.	
Rights Administrator	An employee of the participant Organization that is authorized to perform the face-to-face proofing of participant individuals requesting an <i>IESO</i> User Account and submitting Online <i>IESO</i> registration information for the granting, change, and revocation of all user accounts and system access privileges required for access to <i>IESO</i> -secure Web servers for people within their own organizations. As a trusted entity in the <i>IESO</i> Identity	

Title	Description	
	Management, a Rights Administrator attests to the <i>IESO</i> that the Individual Subscriber or Application Subscriber is who they say they are.	
Individual Subscriber	Individual that works for a participant Organization that interacts with one or more of the <i>IESO</i> information systems and possesses an <i>IESO</i> User Account for individual use or submits <i>IESO</i> identity and system access management requests regarding an <i>IESO</i> User Account via the Rights Administrator.	
Application Subscriber	An individual that works for or represents a participant Organization and is responsible for managing an <i>IESO</i> User Account assigned to an application (i.e. Machine/API accounts). Possesses an <i>IESO</i> User Account for application use (custodian) or submits <i>IESO</i> identity and system access management requests regarding an <i>IESO</i> User Account.	
<b>General Terms</b>		
Credential Subscriber	General term for any <i>IESO</i> identity management end entities. Any entity who applies for or possesses any type of identity credential	

– End of Section –

## 3. Identity Trust Operational Model

---

### 3.1 IESO Trust Model

The trust model is an abstract delegation construct by which the IESO assigns access rights to persons to connect to and use information and systems provided by the IESO, while maintaining the ability to hold those persons legally accountable for misuse or misconduct with those access rights.

We maintain this trust model to protect against two types of risk:

- 1) Use of granted access rights causes harm to the *IESO*, another participant, or any stakeholder of the *IESO* Administered markets. The ability to legally seek redress is the mitigation of this risk.
- 2) Use of granted access rights causes harm to the participant organization itself. The trust model and the audit records we keep of the trust model protect *IESO* against legal liability from the organization for misuse of access rights.

From before market opening in May 2002, the *IESO* has maintained a trust model to delegate access rights. The original trust model was supported by technical controls provided by expensive and administratively burdensome Public Key Infrastructure (PKI) technologies. The use of PKI technologies was discontinued in 2012 which reduced costs extensively, but administrative burden to a lesser degree. The roles associated with the obsolete PKI trust model were essentially continued although the processes to grant and revoke access rights remained quite manual.

With updated registration processes including automated account provisioning, the IESO is further enabling business process automation and removing more of the administrative burden for the participants. Further automation within the Online IESO BPMS tools for actual account provisioning direct to and by account holders instead of manual creation and communications will realize same day account issuance for most end users.

In the updated trust model for management of access rights, Authorized Representatives are still at the top of the hierarchy, next are Primary Contacts, next are Rights Administrators, and last are the custodians or holders of an account with rights to access information held by the IESO or exercise functionality offered by IESO systems.

Authorized Representative is a role given to persons who have the authority to legally bind their organizations. This role group is established for the *Participant* when the Participation Agreement is signed, and the signatory becomes the first and original Authorized Representative for their organization. The Authorized Representative may, and is encouraged to, delegate additional Authorized Representatives so that a single individual departing the organization does not leave the Authorized Representative role group for their organization empty, thus breaking the trust model and the risk mitigation that provides. Should this happen, a new first and original Authorized Representative must be established for their organization, and the IESO requires a letter and signature of this person to accomplish this.

Authorized Representatives have one specific responsibility in the trust model, and that is assigning Primary Contacts for their organization. Primary Contacts have the responsibility to be the primary point of contact between the IESO and their organization, but within the trust model, their primary responsibility is to assign Rights Administrators and assign additional Primary Contacts. The

Authorized Representatives will be asked to establish new Primary Contacts should the Primary Contact role group become vacant for an organization.

Rights Administrators have responsibilities entirely within the scope of the trust model. Those responsibilities are to assign access rights to persons to connect to and use information and systems provided by the IESO. The scope of access rights available to be assigned are defined by the IESO, and entirely based upon the market, program and service provider participations requested by or authorized to that organization. The Primary Contacts will be asked to establish new Rights Administrators should the Rights Administrator role group become vacant for an organization.

Custodians of accounts have responsibilities to conduct the business of their organization and the IESO using the access rights assigned to the accounts they hold. Their responsibility in the trust model is to neither share their account or the account's credentials nor the misuse the account to cause harm to their organization, the IESO, or stakeholders of the IESO.

## 3.2 Identity Proofing

There is no requirement by the *IESO* for identity proofing of Primary Contacts, Rights Administrators or persons acting in other roles although it is prudent that *participants* do so.

It is up to the *participant* to determine and employ the identity procedures that best fits within their own policies. Identity proofing an individual is the process of authenticating that an individual is who he or she claims to be. The process for determining that an individual is who he/she says he/she is may vary, but a generally accepted and recommended practice is for the *participant* to compare at least two of the individual's credentials with the physical characteristics of the individual in a face-to-face meeting. An example of this would be for the independent individual to review the Passport and Driver License of the individual and compare the photos with the person present. Additionally, the independent party may ask the individual to sign his name and compare the signed signature with the one on the Passport and Driver's License.

## 3.3 Rights Administrator Model

**This model is the only one currently and going forward. Its continued use via the Online IESO Registration system reduces administrative overhead for all concerned.**

In this model the *participant* has an employee that is authorized as the Rights Administrator to manage user accounts of Individual Subscribers or Application Subscribers (Custodian person). A Primary Contact is an employee of the *participant* responsible for validating the identity and credentials of Rights Administrator and registering that person in that role for the *participant* via the Online IESO Registration system.

Individual Subscribers and Application Subscribers applying for a User Account will do so via the Rights Administrator who will use the Online IESO Registration system to submit a request for user accounts for those persons and initiate automated account provisioning with the IESO's current authentication system provider - Okta.

The Rights Administrator is responsible for handling all user account requests other than Primary Contacts and Authorized Representatives and email based IESO Workspaces accounts. This includes the User Account issuance and system access role requests, user credential changes and deactivation requests and User Account password reset requests. However, end users can and should use the Online IESO Registration system to manage their own account attribute changes such as last name, email address and phone number.

**– End of Section –**

## 4. Identity Management Procedural Work Flows

The following diagrams represent the flow of work and information relating to the Identity Management procedures among the *IESO*, and external *participant* involved in the procedure.

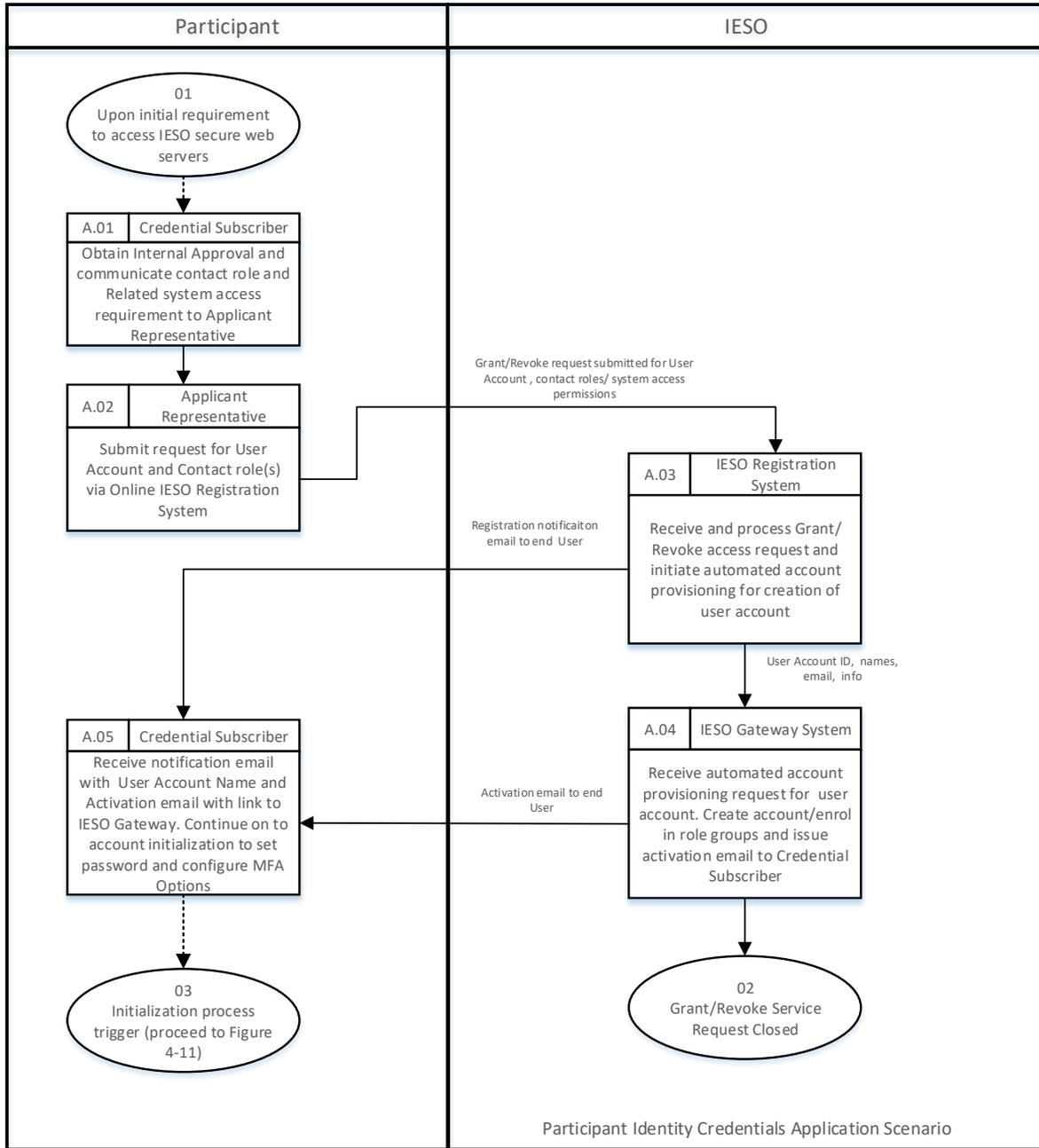
The steps illustrated in the diagrams are described in detail in Appendix A.

**Table 4-1: Legend for Work Flow Diagrams**

<b>Legend</b>	<b>Description</b>
Oval	An event that triggers a task or that completes a task. Trigger events and completion events are numbered sequentially within procedure (01 to 99).
Task Box	Shows reference number, the party responsible for performing task (if “other party”), and the task name or brief summary of the task. Reference number (e.g., 1A.02) indicates procedure number within the current <i>Market Manual</i> (1), sub-procedure identifier (if applicable) (e.g. A, AA), and the task number (02).
Solid horizontal line	Shows the information flow between the <i>IESO</i> and external parties.
Solid vertical line	Shows the linkage between tasks.
Broken line	Links trigger events and completion events to the preceding or succeeding task.

### 4.1 Participant User Account Application Scenario

In this scenario, a *participant* employee or contractor applies for a user account and participant contact roles / permissions via the *participant* Applicant Representative.



**Figure 4-1: Participant User Account Application Scenario**

## 4.2 Participant User Account Change Scenario 1

In this scenario, an existing Individual Subscriber or Application Subscriber applies for a change that does not impact identity credentials directly but does involve granting or revoking one or more participant contact roles and/or system access roles / permissions via an Applicant Representative / Rights Administrator where applicable.

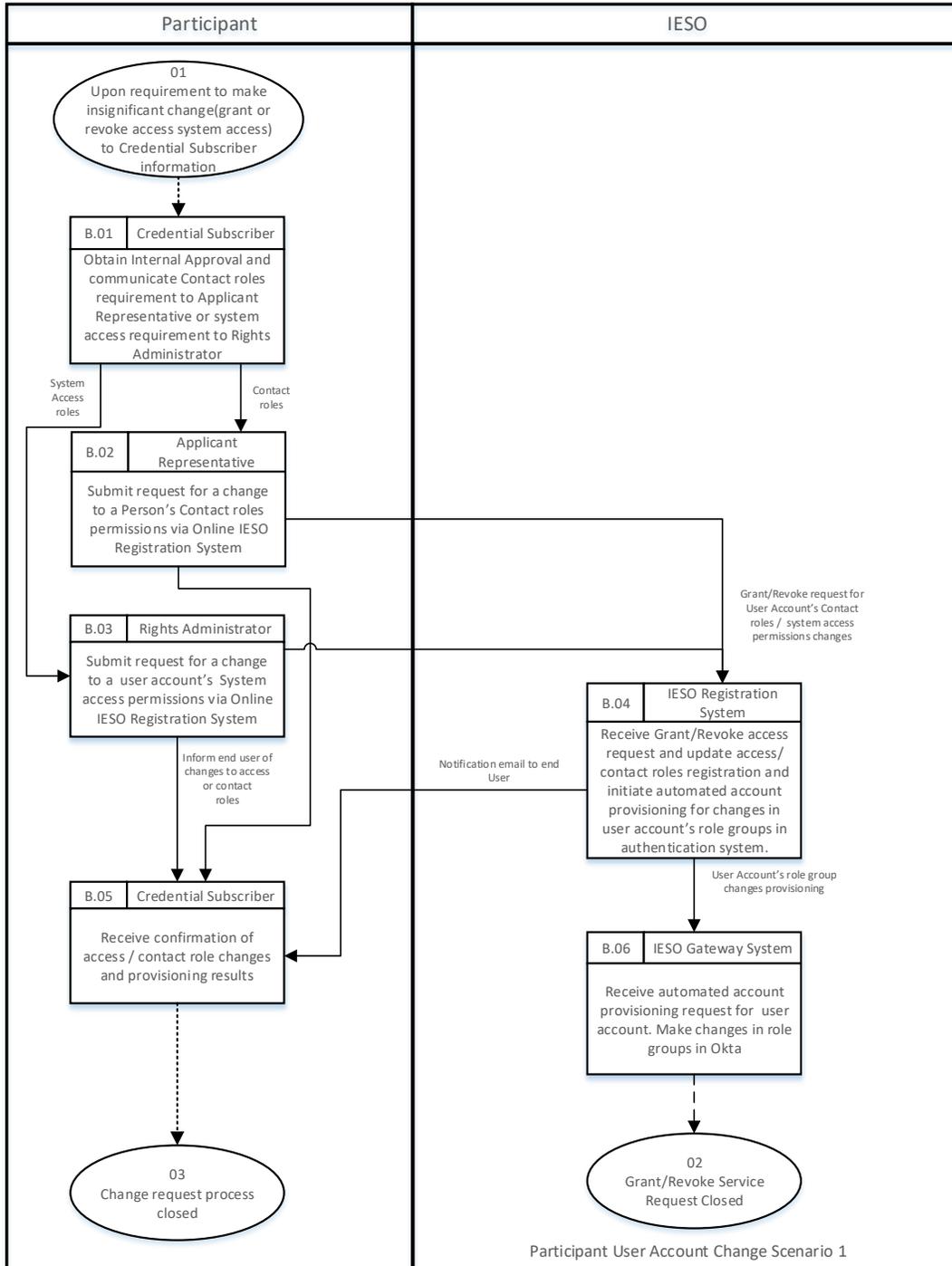
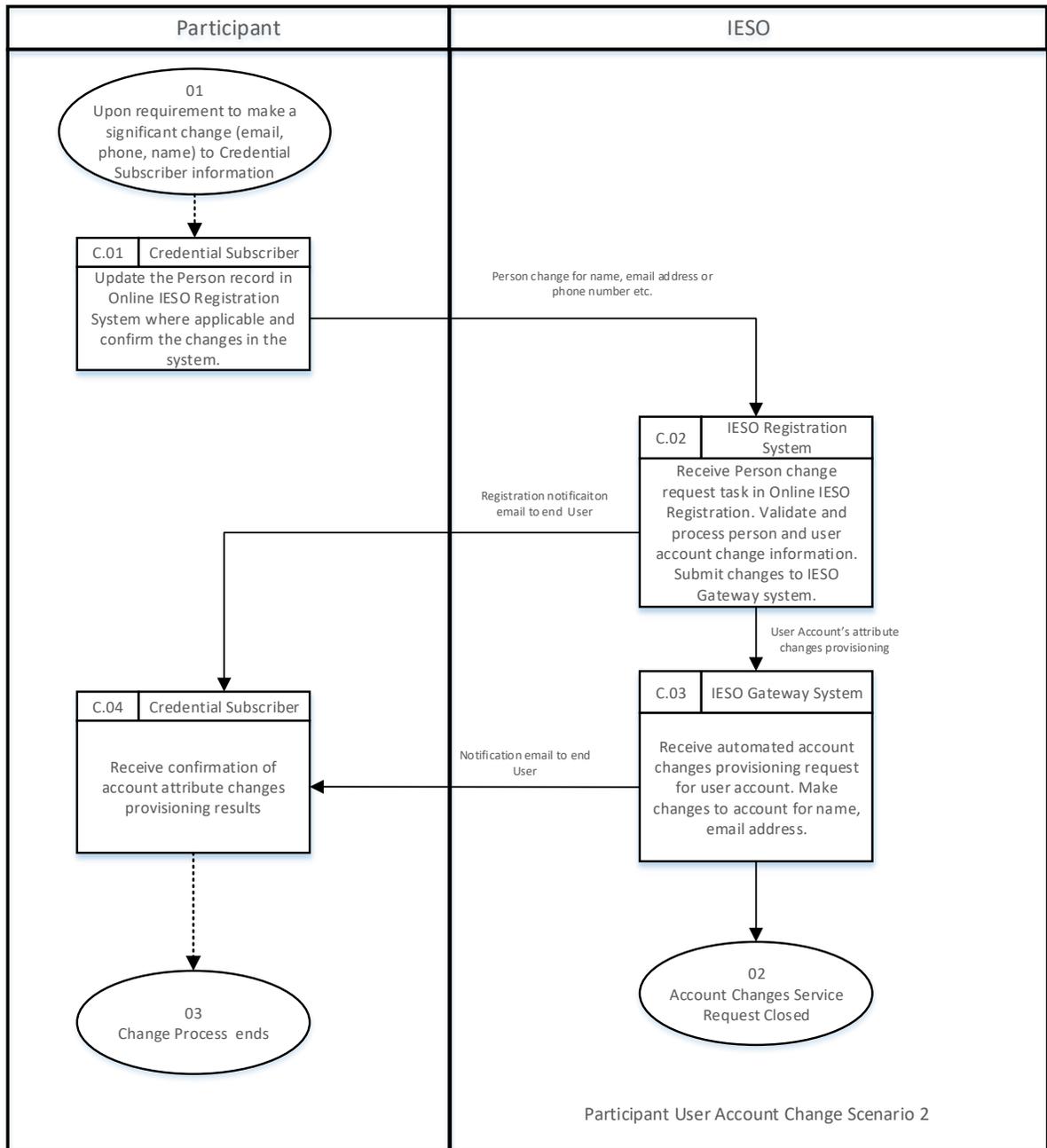


Figure 4-2: Participant User Account Change Scenario 1

### 4.3 Participant User Account Change Scenario 2

In this scenario, an existing Individual Subscriber or Application Subscriber submits ‘person’ record changes that impact the credential attributes for the person’s associated personal or machine user account such as name, machine account custodian name, email address, phone number.



**Figure 4-3: Participant User Account Change Scenario 2**

## 4.4 Participant User Account De-provisioning / Deactivation Scenario

In this Scenario, an existing Individual Subscriber’s or Application Subscriber’s account requires removal of participant contact roles and/or system access roles / permissions and potentially deactivation where it is no longer required and a *participant* Applicant Representative and/or Rights Administrator submit those requests.

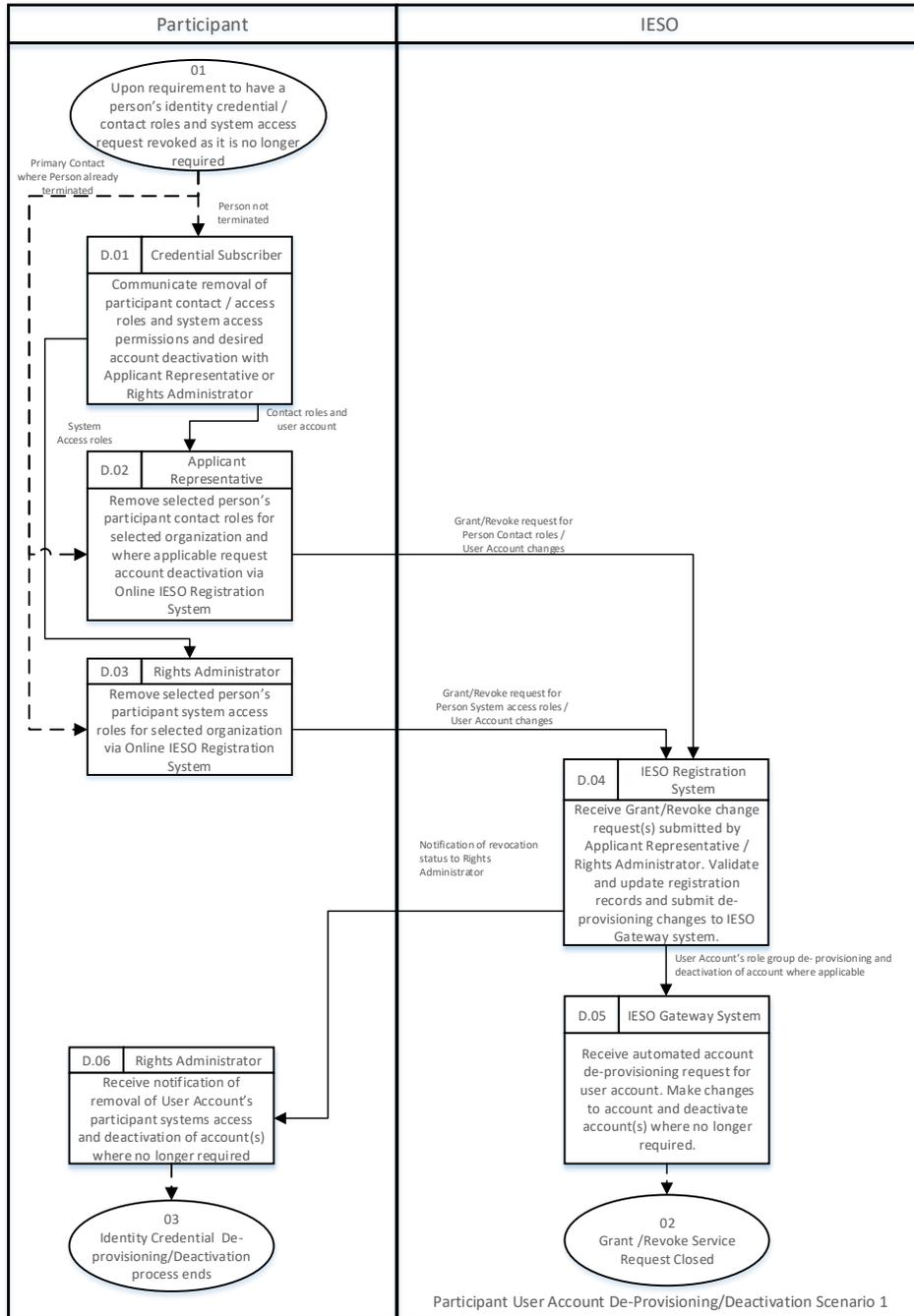
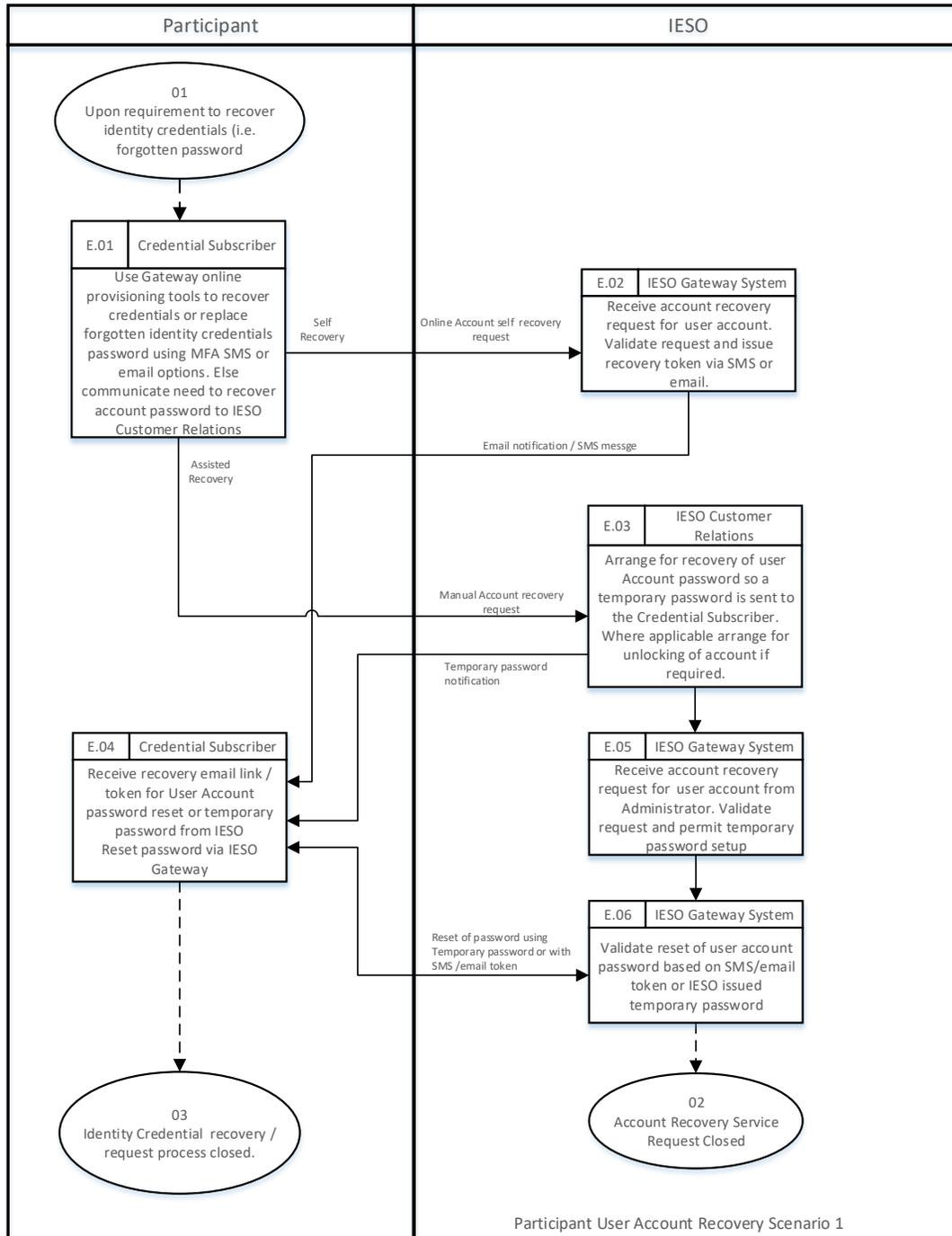


Figure 4-4: Participant User Account De-provisioning / Deactivation Scenario

## 4.5 Participant User Account Recovery Scenario 1

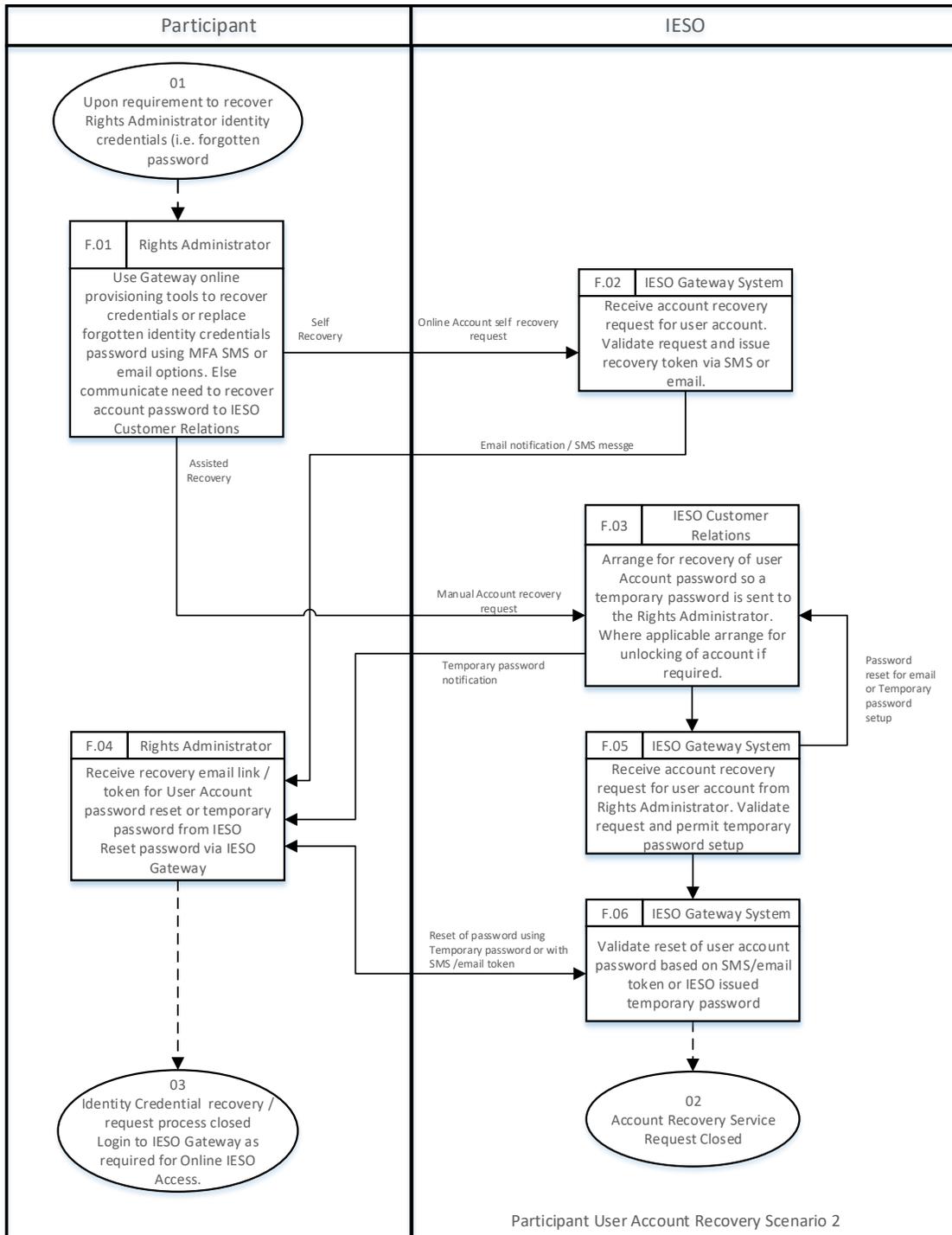
In this scenario, an existing Individual Subscriber or Application Subscriber performs an online recovery of their identity credential or requests the recovery of their identity credential via *IESO* Customer Relations.



**Figure 4-5: Participant User Account Recovery Scenario 1**

## 4.6 Participant User Account Recovery Scenario 2

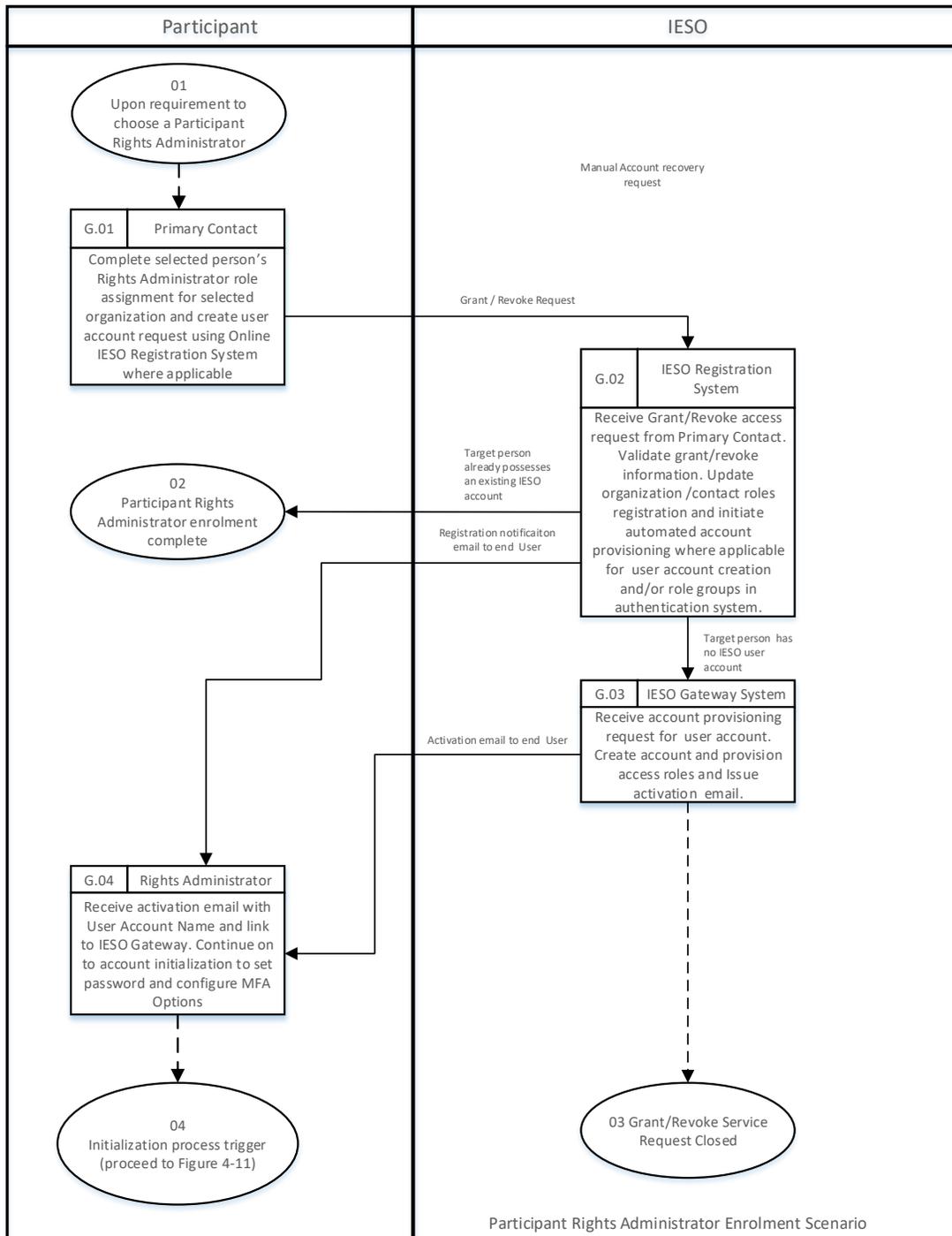
In this scenario, an existing Rights Administrator performs an online recovery of their identity credential or requests the recovery of their identity credential via *IESO* Customer Relations.



**Figure 4-6: Participant User Account Recovery Scenario 2**

## 4.7 Participant Rights Administrator Enrolment Scenario

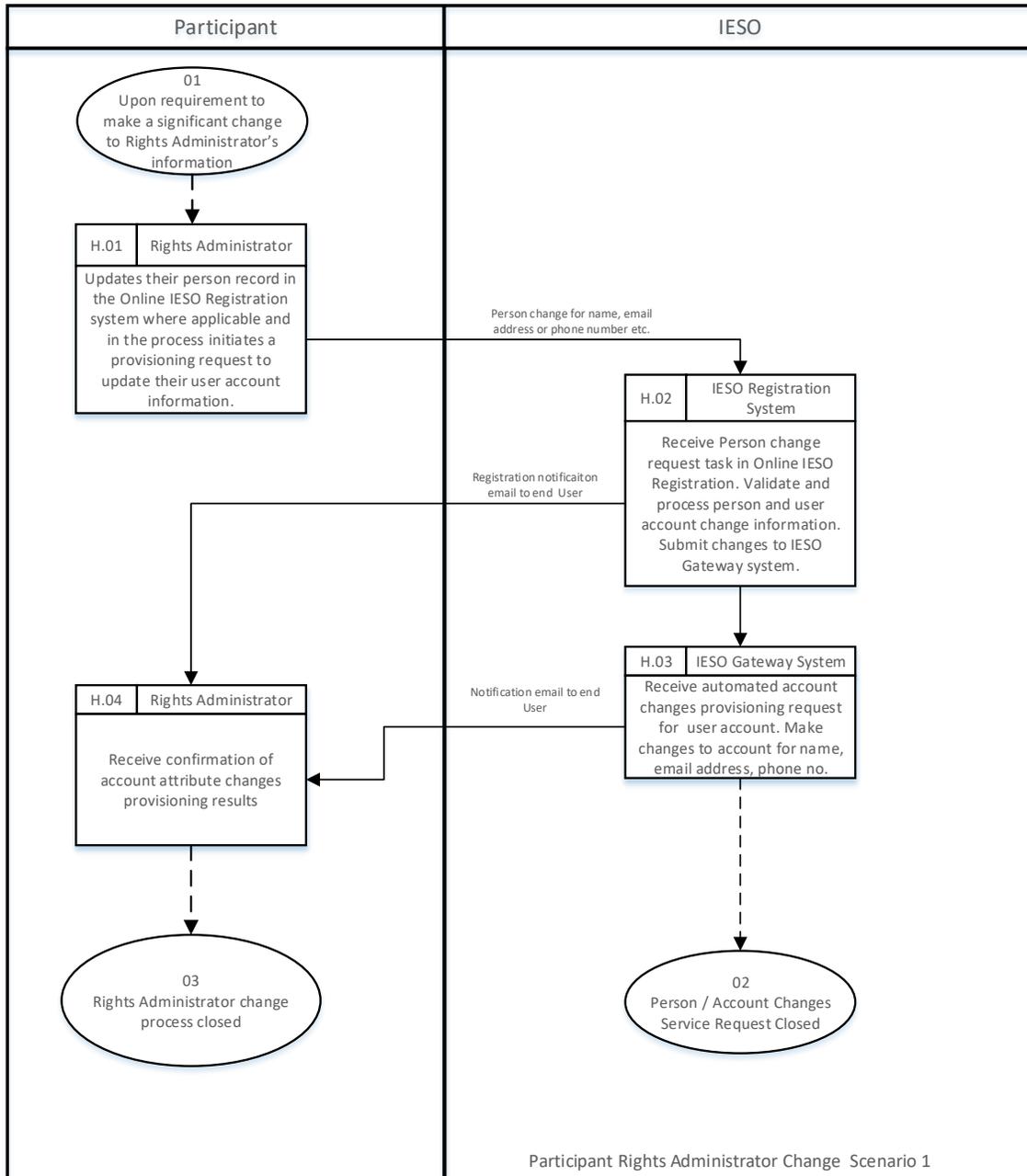
In this scenario, a *participant* Primary Contact requests the Rights Administrator role for an employee in either Sandbox and/or Production environments.



**Figure 4-7: Participant Rights Administrator Enrolment Scenario**

## 4.8 Participant Rights Administrator User Account Change Scenario 1

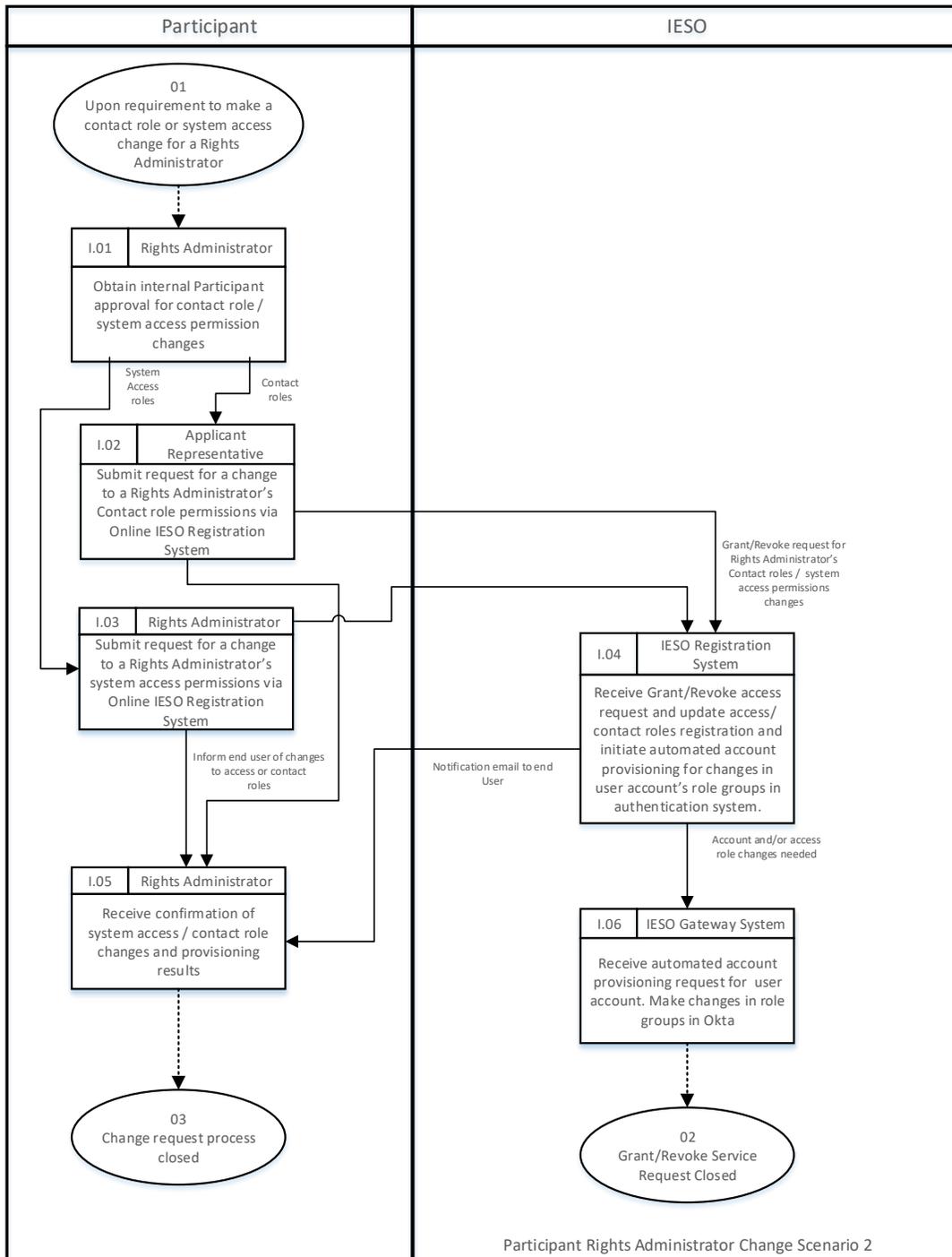
In this scenario, an existing Rights Administrator requests a change that impacts credential attributes for their account such as name, email address, phone number information.



**Figure 4-8: Participant Rights Administrator Account Change Scenario 1**

## 4.9 Participant Rights Administrator User Account Change Scenario 2

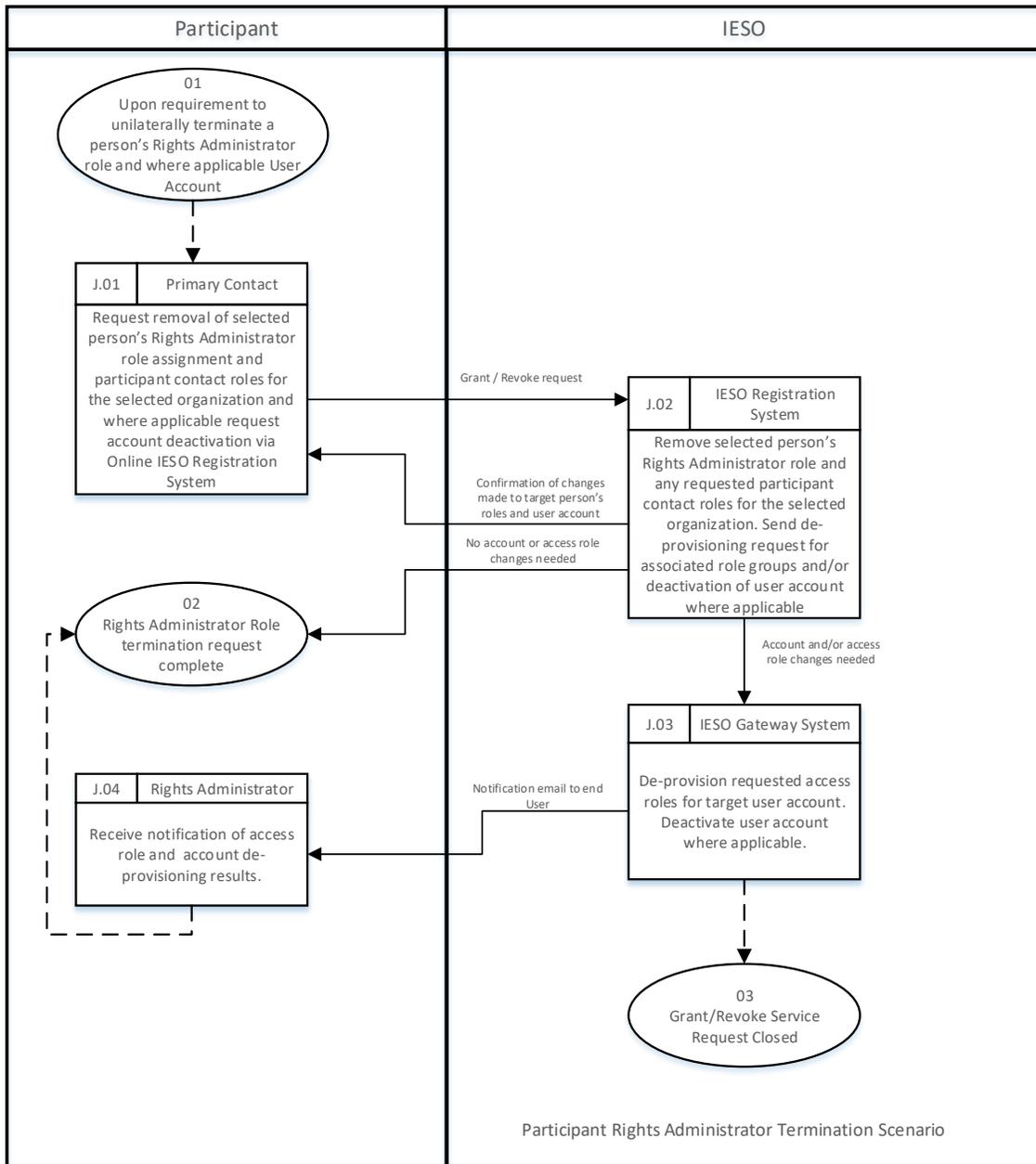
In this scenario, a person in an existing Rights Administrator role requests participant contact roles and/or system access permissions changes for self or another Rights Administrator.



**Figure 4-9: Participant Rights Administrator Account Change Scenario 2**

## 4.10 Participant Rights Administrator Role Termination Scenario

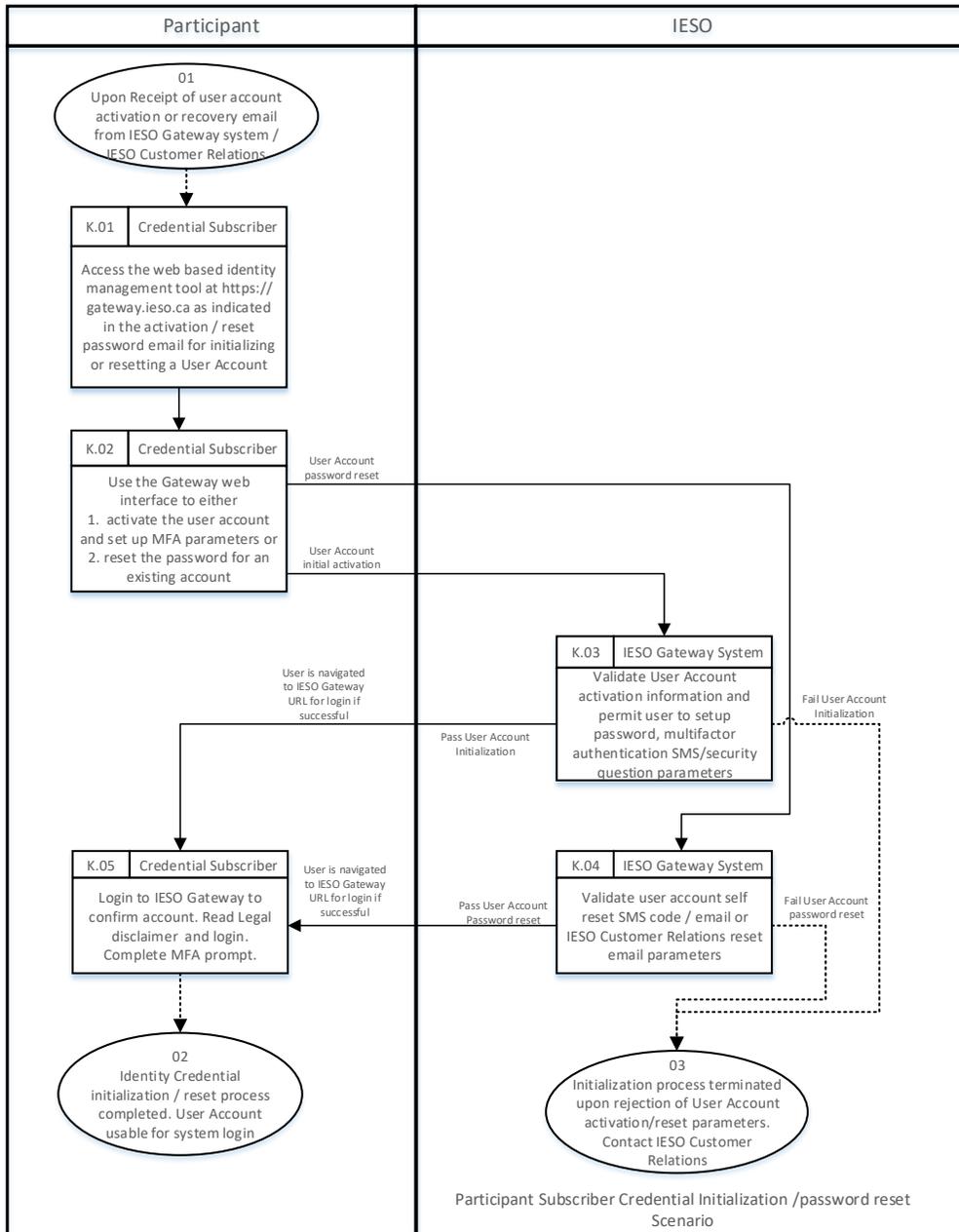
In this scenario, the Primary Contact is requesting the termination of a person’s Rights Administrator role (and specific participant contact roles / system access roles) and where applicable deactivation of the related User Account.



**Figure 4-10: Participant Rights Administrator Role Termination Scenario**

## 4.11 Subscriber User Account Initialization / Password Reset

The following diagram represents the process by which an Authorized Representative, Primary Contact, Individual Subscriber, Application Subscriber or Rights Administrator, etc. can activate their IESO Gateway (Online IESO, Energy Market Interface, Outage Management, TRA, Prudential Manager, Dispatch Service system, Reports site) User Account/Password or reset the password for their account.



**Figure 4-11: Subscriber User Account Initialization /Password Reset**

## 4.12 Periodic Update of Subscriber User Account Password

The following diagram represents the process by which the user account password for any Authorized Representative, Primary Contact, Individual Subscriber, Application Subscriber or Rights Administrator, etc. is initialized or reset when logging in to the IESO Gateway. Password initialization or reset involves password changes to a User Account. After password initialization/reset has been completed successfully the user account may be used to login to the IESO Gateway, Report Site, Energy Market Interface site, Outage Management site, Dispatch Service, Prudential Manager, Transmission Rights Auction, or Online IESO Registration system, etc. where granted access privileges permit. The exception is email based accounts which are specific only to the Online Workspaces system.

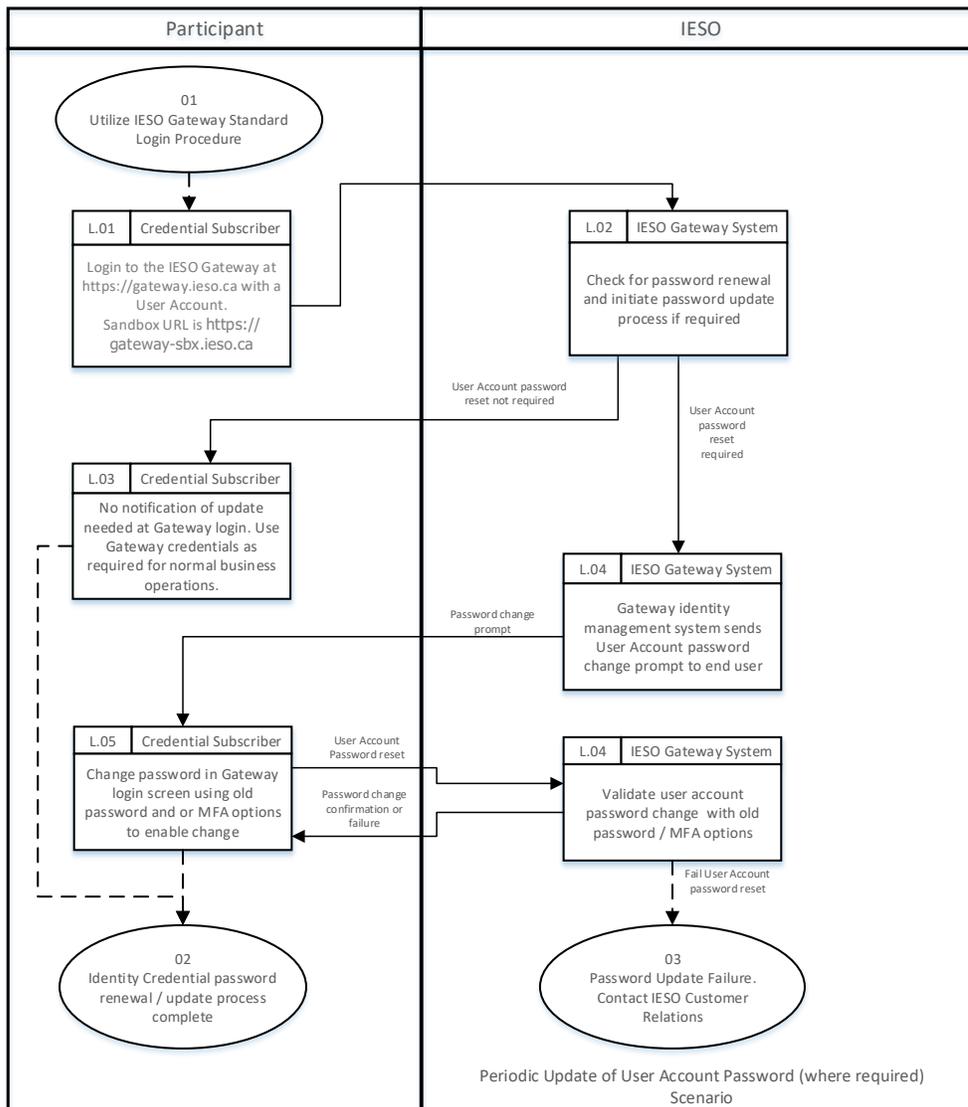


Figure 4-12: Periodic Renewal of User Account Password

- End of Section -

## 5. Participant Primary Contact Operational Guidelines

---

### Section organization:

1. What is a Primary Contact?
2. IESO Trust Model and Identity Credential Proofing
3. Appointing a Rights Administrator
4. Instructions for using the IESO Registration System to Register a Rights Administrator and Request an Account and System Access
5. Requesting a Person's Rights Administrator Role Termination
6. Steps to be Taken When Registering a Rights Administrator for Registration System Access and a User Account.

### 5.1 Primary Contact Definition

The Primary Contact is an officer of a *participant* Organization who is authorized by the Authorized Representative (e.g. Senior Officer) to register Rights Administrators for identity credential services on behalf of the *participant* Organization. The identities of Primary Contacts are communicated to the IESO by the Authorized Representative via the Online IESO Registration System. Typically, this should be done at the time of initial *participant* registration but can be done any time afterwards if missed at that point and it should be done any time a change occurs with a Primary Contact.

The Primary Contact then designates and delegates the role of the Rights Administrator via the Registration system. The term Credential Subscriber generically refers to any person who possesses an IESO User account.

### 5.2 IESO Trust Model and Identity Credential Proofing

*Participants* have just one trust model provided by the IESO. Although not required to do so by the IESO, it is prudent for each *participant* to do their own identity proofing of Rights Administrators, Individual Subscribers and Application Subscribers. Please reference Section 3 of this Guide regarding the trust model and suggested identity proofing.

#### 5.2.1 Participant Rights Administrator

Within the model the *participant* has an employee that will act as the Rights Administrator (See [“Appointing a Rights Administrator”](#) in the section below. Individual Subscribers and Application Subscribers applying for a user account shall go to the Rights Administrator to be proofed and to use the Rights Administrator for all identity credential and IESO system access lifecycle management functions.

### 5.3 Appointing a Rights Administrator

A Rights Administrator is an employee of a *participant* Organization that is authorized to perform the face-to-face proofing of Individual Subscribers and Application Subscribers requesting market

systems access and an *IESO* identity credential. As a trusted entity in the *IESO* Identity Management solution, the Rights Administrator attests to the *IESO* that to the best of their knowledge the Individual Subscriber or Application Subscriber is who they say they are.

The method used in appointing a Rights Administrator is at the sole discretion of the *participant* Organization. The *IESO* make no assertions to the individuals that should be selected. The *IESO* does, however, make the following recommendations on the traits that should be possessed by an individual selected for this Trusted Role:

- Full Time employee of the *participant* and not a Contractor working for the *participant*;
- Be in good standing with the government; and
- Be in good standing with the *participant* Organization.

## **5.4 Process to Register a Rights Administrator and Request an Account and System Access**

See Section 8 on Registering a Rights Administrator and requesting an account and systems access.

## **5.5 Requesting a Person’s Rights Administrator Role Termination**

A Primary Contact can initiate termination of the role for any Rights Administrator entity under their span of control. To gain a better understanding of the process flow for this request, please reference the “Identity Management Procedural Work Flows” section in this Guide.

### **5.5.1 Circumstances for Deactivation of IESO Systems Access and User Account**

Deactivation of the *IESO* Market system access and user account is the process of permanently ending the operational period of a User Account’s system access privileges and the User Account as well where applicable from a specified time forward and not reissuing replacement identity credentials. Some of the suggested reasons for requesting user account deactivation of any *participant* Rights Administrator entity are detailed below, but the Primary Contact may request a deactivation for any reason they deem necessary:

- Organization is in bankruptcy or liquidation
- Affiliation change
- Individual terminates job or
- job responsibilities no longer require *IESO* identity credentials

## **5.6 Steps for Registering a Rights Administrator for Registration System Access and a User Account**

See section 4.7; Participant Rights Administrator Enrolment Scenario.

– End of Section –

## 6. Participant Rights Administrator Operational Guidelines

---

### Section organization:

1. What is a Rights Administrator?
2. Instructions for using the IESO Registration System
3. IESO Trust Model and Guidelines for Proofing Credential Subscribers
4. Guidelines for Form Storage, Protection, and Archival
5. IESO Customer Relations Communications
6. Guidelines for Distributing and Using Identity Credential Activation Data
7. Person ID Number
8. Basic Trouble Shooting

### 6.1 Rights Administrator Definition

The Rights Administrator is an employee of a *participant* who is authorized submits requests for user accounts and system access via the Online IESO Registration system. Throughout this document the term Credential Subscriber refers to the Individual Subscriber and the Application Subscriber (Custodian person).

The Primary Contact shall request an identity credential for the Rights Administrator's use within the Registration system and shall assign the Rights Administrator role to an employee within the *participant*. The same principles and practices apply when issuing credentials to a Rights Administrator as they do when issuing identity credentials to an Individual or Application Subscriber.

### 6.2 Instructions for Using the IESO Registration System

See Section 8 on requesting a user account and systems access for a Credential Subscriber.

### 6.3 IESO Trust Model and Guidelines for Proofing Credential Subscribers

*Participants* have only one trust model provided by the *IESO*. Although not required to do so by the *IESO*, it is prudent for each *participant* to do proofing of Individual Subscribers and Application Subscribers and it is up to the *participant* to determine and employ the identity procedures that best fits within their own policies. This section of the Rights Administrator Operational Guidelines details proofing guidelines that may be used by Rights Administrators but it is up to each *participant* to determine the procedures to be used or not.

### 6.3.1 When should the Identity of a Credential Subscriber Be Proofed

It is recommended that the identity of a Credential Subscriber should be proofed in the following circumstances:

- On initial identity credential issuance request,
- If a Credential Subscriber requesting an identity credential transaction has not previously authenticated his or her self to the Rights Administrator at the *participant*,
- If a Credential Subscriber incurs Significant Change, (see Appendix B for explanation), or
- When deemed necessary by the Rights Administrator.

### 6.3.2 Process to Validate the Identity of the Credential Subscriber

The IESO recommends that a person requesting market systems access and an identity credential transaction on behalf of a *participant* that has not previously authenticated himself to the Rights Administrator should present himself in person to the Rights Administrator along with two pieces of identification. Original or notarized copies should be provided and at least one piece of identification should be photo identification containing the requester's current name and address. Examples of appropriate identification include – Valid Passport, Birth Certificate, Valid Provincial/Territorial Driver's License, Canadian/US/Other Citizenship Certificate, or Organization Identification.

If the Credential Subscriber requesting the transaction has an existing relationship with the Rights Administrator, the Credential Subscriber should authenticate himself to the Rights Administrator by providing evidence of that relationship. Appropriate techniques can include but are not limited to:

- Confirmation of a shared secret
- Answering pre-defined questions that would be difficult for someone else to correctly answer.

The IESO recommends that the Rights Administrator should verify that the relationship is true and in good standing and that the person's original credential information is current. It is prudent that the Rights Administrator retain a record of the original proof of identity of the individual based on internal *participant* documentation practices. The Credential Subscriber should also retain a copy of this and store it in a secure location for future reference. At no time should the copy be available to any other individual except the Rights Administrator.

## 6.4 Guidelines for Form Storage, Protection, and Archival

Although the IESO no longer requires the *participant* to do so, internal *participant* forms or reports used in the identity management process help establish a paper/information trail. As such, it is recommended that forms be maintained with security and protection in mind. Following are recommended guidelines for storing and archiving forms in a secure and protected manner:

- Only authorized *participant* individuals should have access to the completed forms

- Any photocopied original Identity Credentials should be highly secured (The *IESO* suggests that copies of Individual Identity Credentials not be made nor retained by the *Participant*)
- The Rights Administrator should provide the Credential Subscriber a copy of the forms for their own records
- The *participant* should have an organised system for active record retrieval and archived record retrieval
- Active records should be securely locked in a drawer, filing cabinet, safe, or a similarly secured storage location
- It is suggested the *participant* archive forms for a minimum of seven (7) years in a secured and environmentally controlled off-site facility.

## 6.5 IESO Customer Relations Communications

In the event that the Online IESO - Registration system is unavailable or where problems are experienced with such, please contact *IESO* Customer Relations so that they can ensure that any issue with it can be dealt with in a timely manner.

<i>IESO</i> Customer Relations Toll Free Phone Number:	1-888-448-7777
<i>IESO</i> Customer Relations Phone Number:	905-403-6900
<i>IESO</i> Customer Relations Fax Number:	905-403-6921
<i>IESO</i> Customer Relations e-mail:	customer.relations@ieso.ca

## 6.6 Guidelines for Distributing and Using Identity Credential Activation Data

The Credential Subscriber who applies for and receives a User Account credential will receive an activation email which will permit them to setup a password and initial login to the IESO Gateway identity management system used for authentication to market facing applications, or IESO Workspaces system or the IESO Reports site. The activation email link for a User Account credential must first be used to setup a password as well as a security question and choose some multifactor authentication options and then login to the IESO Gateway. The activation email link will cease to do so after 90 days after which, if the account is still required, the user will need to communicate to the IESO for a temporary password. The *IESO* Gateway User Guide details how to initialize a user account.

The same is essentially the same now for the Credential Subscriber (custodian) who applies for and receives an API User Account credential used with the EMI, CROW OCSS, Dispatch Service or Online IESO Web Services or Reports Site (i.e. machine account). She or he will securely receive an activation email from the IESO Gateway system. The custodian will then need to use the activation email link and in the process of doing so setup the password to one of his/her own choosing and set up the associated security question and answer and any IESO configured MFA options. However, the machine account will have no market application access permissions in the IESO Gateway and the custodian can logout. The account can then be used with the MIM, OCSS, Dispatch or Online IESO Web Services or Reports site where registered for such use. The custodian can periodically (on a schedule of his / her own choosing), change the password and security question and answer for the machine account (see the IESO Gateway User Guide for the self service password reset procedure).

### 6.6.1 IESO Personal User Account Credentials

Any User Account credential for an IESO personal user account ID or an email based account shall where feasible be up to an 8-character alpha string generated by the IESO Registration system when used by the Rights Administrator under the following algorithm rules where feasible.

- Up to 8 characters' long
- Up to the first 7 characters shall represent the last name of the user. If the user's last name is greater than 7 characters, then it will be truncated at the 7<sup>th</sup> character
- The 8 character shall be the first letter of the user's first name. (i.e. Users "Jim Jones" and "Steve MacMasterly" would have user accounts "jonesj" and "macmasts" respectively)

If the user account already exists for a different person, then the up to the first 6 characters will represent the user's last name and the 7<sup>th</sup> and 8<sup>th</sup> characters will represent the initials from the user's first and second name. (I.e. Users "Jim L. Smith" and "John H. Smith" would have user accounts "smithjl" and "smithjs" respectively. If users "Jim Smith" and "Jim. Smith Jr. exist, user accounts "smithj" and "smitji" would be created.) The user profile information in the identity management systems would be populated to accurately reflect the differences.

Any User Account credential for an *IESO* machine/application account shall be a variable character alpha string generated automatically by the *IESO* Registration system under the following algorithm rules.

- The first 6 characters shall be APIIESO to clearly identify the account as a machine account used for IESO systems. For Sandbox accounts SAPIIESO.
- This shall be followed by up to 5 numeric characters. Each new API account will have the numeric component incremented so that the account ID is unique.

Existing API accounts manually generated before use of the Online IESO Registration System will remain as they are.

The Online IESO Registration system will use automated account provisioning in conjunction with the IESO Gateway system (based on Okta) for creating the account or granting system access privileges. The IESO Gateway system will create the User Account and will via an activation email, send the account information directly to the Credential Subscriber based on the email address provided by the Rights Administrator in the Registration system. It is critical to the trust model employed within the Online IESO Registration system and identity management solutions that the email address for the Individual or Application Subscriber (custodian) be current and accurate.

However, in the event that the email address is, incorrectly defined by the Rights Administrator within the Online IESO Registration system and no activation email is received, the Credential

Subscriber should contact the Rights Administrator to make a correction to ensure in the delivery of the User Account to the Credential Subscriber by registering the correct email and follow up with IESO Customer Relations.

## 6.6.2 User Account Password Reset

Any User Account credential for an *IESO* user or machine account used with the IESO Gateway, Report Site, Energy Market Interface, CROW Outage Management system, Dispatch Service, TRA, Prudential Manager, Online IESO system, or any Web Service or the IESO Workspaces system where needed can have its password self reset by the end user via the Gateway login pages.

In cases where there are problems doing so the end user can request to have their password reset by IESO Gateway authentication system via IESO Customer Relations.

Where applicable only two methods will be used for reset of the password for the Credential Subscriber; password reset email or a temporary password provided to the end user. Throughout the entire process, knowledge of the password / email must be kept solely between IESO Customer Relations and the Credential Subscriber. Once the email or temporary password has been received by the Credential Subscriber, he/she can login to the IESO Gateway Identity Management system with that User Account and one-time password or use the password reset email and reset their password as required.

The Credential Subscriber should have already chosen an appropriate MFA method and security question and appropriate answer for password self-recovery and extra authentication purposes as well.

Passwords have the following rules.

- At least 8 characters' long
- Case sensitive
- Require a mix of both upper and lower case alpha and numeric characters
- Allow special characters (various forms of punctuation and other symbols)
- No parts of your username

Other rules for User Account passwords include the following:

- Passwords shall not be stored in clear text
- Password histories shall be maintained for each user or machine account. The user should not be allowed to reuse any of the last four passwords.

## 6.6.3 Delivery of Password Reset Email

There might be a situation where an end user cannot recover their own password and will need to have it reset by an IESO Administrator.

**\*\*Please note: This option should only be considered after attempts to follow the Self Service Password Reset have failed.**

In order to initiate the “Password Reset by Administrator” process, the end user must start by sending an e-mail requesting a password reset to [customer.relations@ieso.ca](mailto:customer.relations@ieso.ca). They should include as much details as possible in this e-mail but at minimum they must include either:

1. The end user's E-mail Address associated with their IESO Gateway (Okta) Account which should match the one registered for the end user.

OR

2. Their IESO Gateway (Okta) UserID (if applicable)

This way the administrators will be able to assist the end user as quickly and as efficiently as possible. Once the Administrator resets the end user's password, they will receive an e-mail with a "Reset Password" button. If an end user receives this e-mail, they can perform the steps shown in the IESO Gateway User Guide in order to reset their password or see section 9 of this document.

#### **6.6.4 Delivery of Temporary password from Customer Relations**

Direct delivery involves delivering the password directly from an IESO IT Administrator to the Credential Subscriber as follows:

- By Phone

IESO Customer Relations will phone the Credential Subscriber to deliver the temporary / reset password to the Credential Subscriber validating that they are talking with the correct individual at the time. The phone number will be captured during person registration in the Online IESO system. After receiving the temporary password, the end user can use the procedure as defined in the IESO Gateway User Guide to set a permanent password.

It shall be the responsibility of each person to maintain correct phone and email information in their person record and in their user account. General company phone numbers alone should not be used for registration or for user accounts. Extensions where applicable should be registered. The Online IESO Registration system will permit each person to login with their user account (once it is created) and perform updates to this information. The system will maintain a historical record of all changes.

### **6.7 Person ID Number**

Online IESO Registration of people for a *participant* will automatically assign a unique person ID number to each person when that person record is first created. This will enable distinguishing one person with the name of John Smith from another person with the same name for example. Each person will be able to see their own Person ID number in the Registration system within their person record but they will not be able to alter it.

During the Initial Issuance process for identity credentials, the Rights Administrator, for each Credential Subscriber, will ensure via this Person ID number that they are requesting a User Account for the intended person. The User Account record stored on the system will be linked to the intended person record to ensure future transactions for user system access are correctly processed.

### **6.8 Basic Trouble Shooting**

For situations that require trouble shooting, please contact *IESO* Customer Relations.

– End of Section –

# 7. Credential Subscriber Operational Guidelines

---

## Section organization:

1. Introduction
2. IESO Trust Model and Identity Credential Proofing
3. Protection of Identity Credential Activation Data
4. Person ID Number
5. Password Creation Guidelines
6. Applying for an IESO Account
7. IESO Systems Access Requests
8. IESO Account Deactivation
9. IESO Account Change
10. IESO Account Recovery

## 7.1 Introduction

These guidelines are meant to supplement Sections 8 and 9 of this Guide to help the Individual Subscriber and the Application Subscribers through the identity credential lifecycle process. Throughout this document the term Credential Subscriber refers to the Individual Subscriber or the Application Subscriber (Custodian person).

To interact with *IESO* Gateway, Online IESO, Energy Market Interface, CROW Outage Management system, Dispatch Service, Transmission Rights Auction, Prudential Manager, IESO Reports Site or other secure IESO Web servers, individuals require an *IESO* identity credential (i.e. a User Account / Password). Please reference section 1.4.2 User Account Identity Credentials of this Guide for more information on identity credentials.

Before receiving an *IESO* identity credential, it is recommended *participant* individuals be positively identified through a secure method of authentication by the *participant* Rights Administrator, as the individual or application account is bound to the appropriate identity credential issued to them. Each identity credential will be registered to an individual person (Individual Subscriber or Application Subscriber).

A User Account is assigned to an individual (person) or application (custodian). Where it is assigned to an application, the Application Subscriber (a.k.a. Application Custodian) is the point of contact even though it may be used by others within the context of machine to machine communications.

## 7.2 IESO Trust Model and Identity Credential Proofing

*Participants* have just one trust model provided by the *IESO*. Although not required to do so by the *IESO*, it is prudent for each *participant* to do identity proofing of Credential Subscribers. Please reference Section 3 of this guide regarding the trust model and suggested identity proofing. Within

this trust model the Credential Subscriber shall communicate with the Rights Administrator to obtain a User Account and request system access privileges.

### 7.2.1 Participant Rights Administrator

In the trust model, the *participant* has an employee that will act as the Rights Administrator. Individual Subscribers and Application Subscribers applying for an identity credential shall go to the Rights Administrator to be proofed and to use the Rights Administrator as the liaison between the *IESO* and the individual for identity credential lifecycle management functions.

## 7.3 Protection of Identity Credential Activation Data

Activation Data is the data required for accessing the User Account or other *confidential* data; examples of Activation Data include passwords, access codes, biometric authenticifiers, and the authorization code. In the *IESO* implementation Activation Data is required to use a User Account.

The Activation Data required to activate the User Account is a password. The password must be input any time that the identity credential needs to be used.

All Activation Data shall be unique and unpredictable, and of strength appropriate for the information it is protecting. All Activation Data should be generated and installed by the Credential Subscriber in their exclusive custody.

## 7.4 Person ID Number

Online *IESO* Registration of people for *participants* will automatically assign a unique person ID number to each person. This will enable distinguishing one person with the name of John Smith from another person with the same name etc. Each person will be able to see their own Person ID number in the Registration system within their person record but they will not be able to alter it.

During the Initial Issuance process for identity credentials, the Rights Administrator, for each Credential Subscriber, will ensure via this Person ID number that they are requesting a User Account for the intended person. The User Account record stored on the system will be linked to the intended person record to ensure future transactions for user system access are correctly processed.

## 7.5 Password Creation Guidelines

Passwords for all identity credentials are case sensitive (The "Caps Lock" key should be off) and must meet the following rules:

- Eight characters or longer, (longer is preferable)
- Contains the following distinguishing features:
  - Upper-case
  - Lower-case
  - A numeric character
  - Special character (punctuation and other symbols). Do not use ampersand &, backslash \, less than symbol <, greater than symbol >, single quote ‘, double quote “
- Includes no spaces
- No parts of the UserID, username
- Not a reused password from the last 4 stored in history

Passwords should not be made up of words that appear in any dictionary or contain the user's name or User Account.

Passwords should not be easy-to-guess as an easy-to-guess password increases the chances that an attacker can gain access to the private key protected by that password and represent him as a valid user.

## 7.6 Applying for an IESO Account

In order to apply for Market Systems access and an account the Credential Subscriber should obtain the proper internal approvals and communicate their requirement to the *participant* Rights Administrator or Applicant Representative within their Organization. Once the Initial Issuance process has been completed the Credential Subscriber will receive an email of the User Account name (i.e. UserID) created and an activation email from the IESO Gateway system. It shall be the responsibility of each person to maintain correct phone and email information in their person record in the Registration system going forward. The Registration system will permit each person to login with their user account (once it is activated and created) and perform updates to this information. The system will maintain a historical record of all changes.

Please refer to Section 9 of this Guide or the *IESO Gateway User Guide* for instructions on how to use a User Account's activation email or temporary password.

## 7.7 IESO Systems Access Requests

All grant or revoke requests regarding *IESO* systems access privileges shall be communicated to an authorized *participant* Rights Administrator or Applicant Representative along with the appropriate internal *participant* approval for such. The Rights Administrator / Applicant Representative will use the Online IESO Registration System to request the user's account be granted or revoked membership in the appropriate participant contact roles or access role groups regarding the targeted systems access. Contact roles' access rights typically are enabled immediately within the Online IESO Registration system. The Registration system will record the user's systems access privileges changes in the IESO master database and an automated provisioning workflow will be created where required by the Registration system to the *IESO* Gateway system to add or remove the user's account in the authentication system's access role groups and notification of the enrolment change will be sent back to the Rights Administrator and also to the Credential Subscriber via email.

## 7.8 IESO Account Deactivation

All requests for *IESO* account deactivation should be communicated to the *participant* Rights Administrator.

### 7.8.1 Account Deactivation

Account deactivation is the process of permanently ending the operational period of an account from a specified time forward and leaving the User Account in a deactivated state. Some of the suggested reasons for requesting a deactivation of any *participant* entity are detailed below.

- Organization is in bankruptcy or liquidation
- Compromise or suspected compromise of a User Account
- Affiliation change of the entity
- Account is superseded

- Individual terminates job or job responsibilities no longer require an *IESO* account
- Whenever any other circumstances or reasonable care would require that an account be deactivated / revoked.

## 7.9 IESO Account Change

All requests for an identity credential change should be communicated to the *participant* Rights Administrator.

An identity credential Change request is required if the Subscriber currently has a User Account for use within the *IESO* Gateway system, Reports site, Online *IESO* Registration system, Prudential system, Energy Market Interface, Outage Management System, TRA system or MIM, Dispatch or OCSS web services and the user account attributes have become inaccurate (e.g. name change, email address change, phone number change) or system access requirements have changed.

## 7.10 Account Recovery

All requests for User Account ‘forgotten password’ reset that the users (or custodian for machine accounts) cannot reset themselves online via the *IESO* Gateway system with their self-chosen MFA options (SMS or email verification or security question and answer) should first be communicated to the *participant* Rights Administrator. However, forgotten User Account password reset requests may be communicated verbally or via email to the *IESO* Customer Relations contact where required. Sufficient user verifying information (i.e. account information, Person ID number etc.) must be provided by the user to sufficiently identify the request as genuine and enable password reset, otherwise the request will be denied.

Once a User Account and temporary password or a password reset email is communicated to the Credential Subscriber, the user can log on to the *IESO* Gateway system and change their password if and where applicable.

– End of Section –

## 8. Use of the Online IESO Registration System

---

### 8.1 Introduction

*Participants* shall be able use the web based Online IESO Registration System to establish the identity of Authorized Representatives, Primary Contacts, Rights Administrators, Individual Subscribers and Application Subscribers, assign them to specific Contact roles and request User Accounts for all. *Participants* maintain the trust model described in section 3 via the use of the Registration System. This must be done independently in both Sandbox and Production Registration systems as required by *Participants*. The choice of who to register in the Sandbox and Production Registration systems is up to each *Participant*.

Once one or more Authorized Representatives for a *participant* have been established any one of them can login to the Registration System to define and designate persons in the role of Primary Contact who in turn can define and assign persons in the role of Rights Administrator. The steps shown below apply to the Rights Administrator role for requesting user accounts and systems access for other users.

The *IESO* makes a distinction between ‘Person’ and ‘User Account’ in its systems. Within the Registration System a person record represents an individual person and the data within the records for that person define who they are. A person’s data such as name, email address, phone number etc., may change over time and this can be updated in the Registration system. A person’s relationship with one or more organizations in various *participant* contact roles may exist over time as well. A User Account record however defines the electronic identity credentials that a person may be associated with and a user account is categorized as either a Personal account or a Machine account as define in Section 7.1. A person’s record may be associated to one or more personal or machine accounts in the Registration system and in addition a person’s personal or machine user account(s) may be associated to one or more *participant* contact roles or system access roles for various *participants* over time as required. Rights Administrators will use the Registration system to define unique Person records and request user accounts for each person.

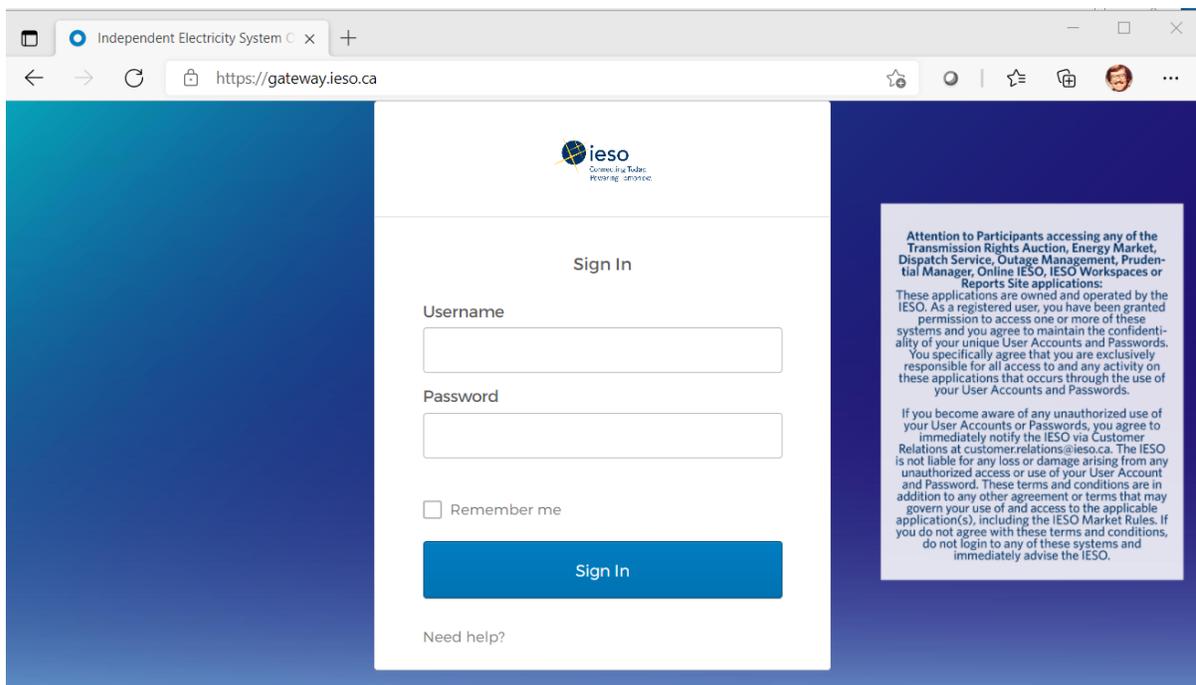
### 8.1.1 Login to the Online IESO System

All *participant* Organization Applicant Representatives, Contacts and Rights Administrators can access the Online IESO system by first navigating to the IESO Gateway system (either Sandbox or Production environment) <https://gateway.ieso.ca> (The Sandbox URL is <https://gateway-sbx.ieso.ca>) to access the login page as shown in Figure 8-1.

Ensure that they are using the IESO supported browser and operating system as listed on the Supported Client Platform page available on the IESO Corporate website at: <https://ieso.ca/en/Sector-Participants/Supported-Client-Platforms>.

The IESO legal disclaimer will be displayed on the login page as shown

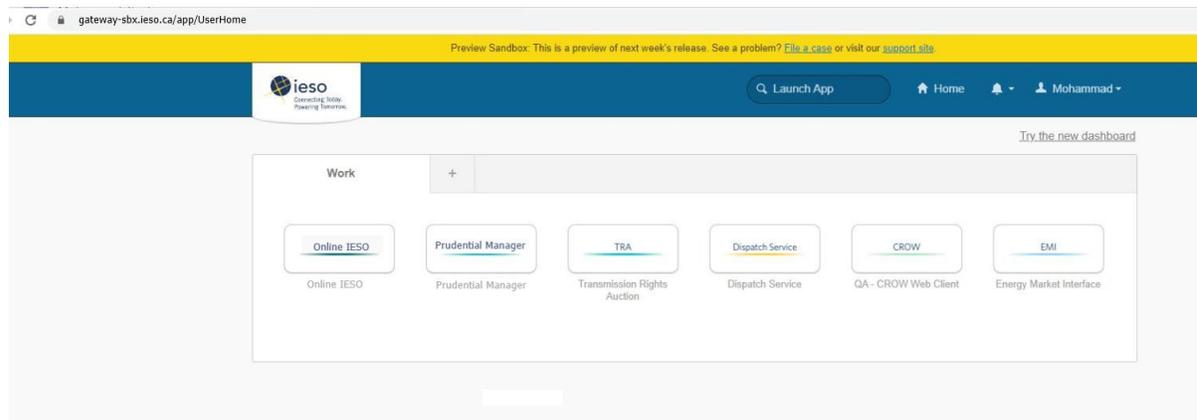
Note that this section shall not deal with other market application functionality now available in Online IESO other than for registration identity and access permission processes.



**Figure 8-1: IESO Gateway Login Page with Legal Disclaimer**

The person's Sandbox and/or Production user account is common for all applications including Online IESO Registration systems in each environment but the same account/password instance is not used between Production and Sandbox environments.

Once logged in, the link in each Gateway environment will navigate the *participant* user to the associated Sandbox or Production Online IESO Registration system as shown in the example in Figure 8-2



**Figure 8-2: Gateway System Landing Page Example**

The “Need help signing in?” link on the Gateway login page will navigate the user to the corresponding help page (Sandbox or Production) where she or he can attempt to recover the password. See Section 9.1.2. The person’s Sandbox and/or Production user account is common for all applications within the IESO Gateway including the Online IESO - Registration system in each environment but the same account/password is not used between Production and Sandbox.

## 8.1.2 Online IESO - Registration Application Actions

### Applicant Representative

Successful login to the IESO Gateway and then navigating to the Online IESO system by an Applicant Representative will take them to an ‘Actions’ page as shown in Figure 8-3.

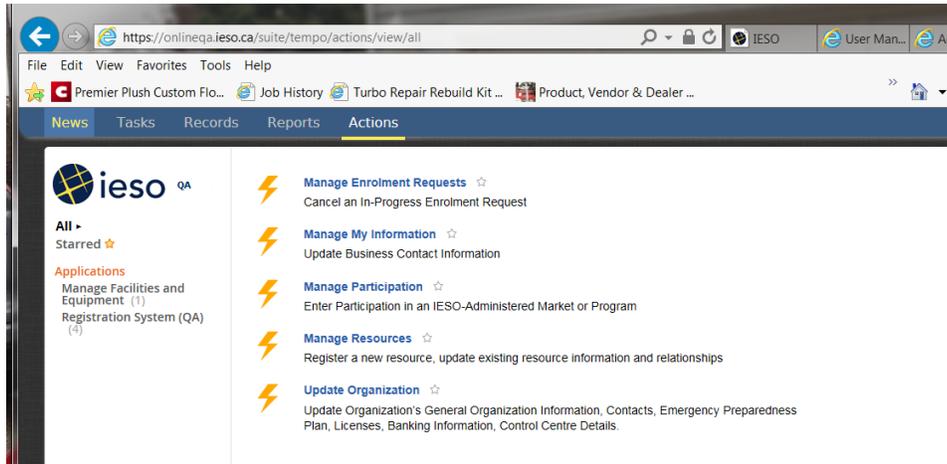


Figure 8-3: Online IESO Applicant Representative - Actions Page

He or she can choose to update their own personal contact information, Manage Enrolment requests, Manage Participations, Manage Resources (i.e. user- resource relationships) or Update Organization (i.e. contacts etc.).

### Participations

The Applicant Representative can choose “Manage Participation” to begin a process instance for requesting participation for their organization from one of those listed in Appendix C. This will impact what contact roles can be requested for various individuals at the participant. Once ‘Manage Participation’ has been chosen the Applicant Representative will be presented with the page to choose the type of Participation as shown in Figure 8-4.

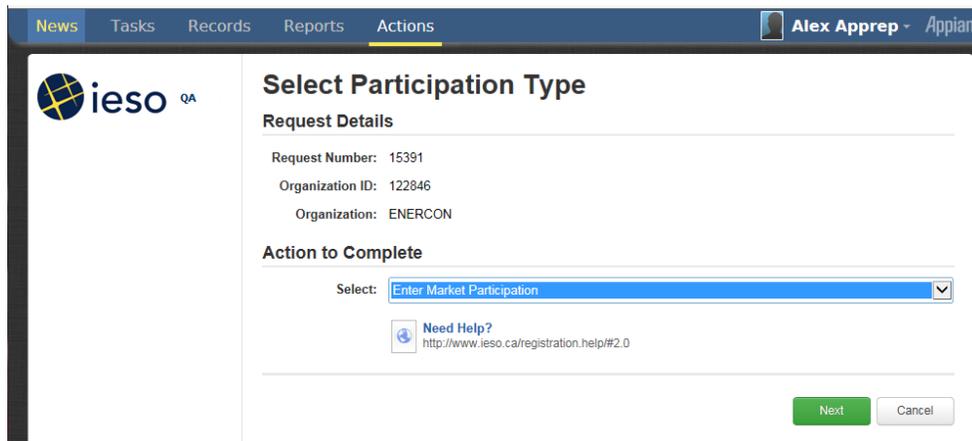


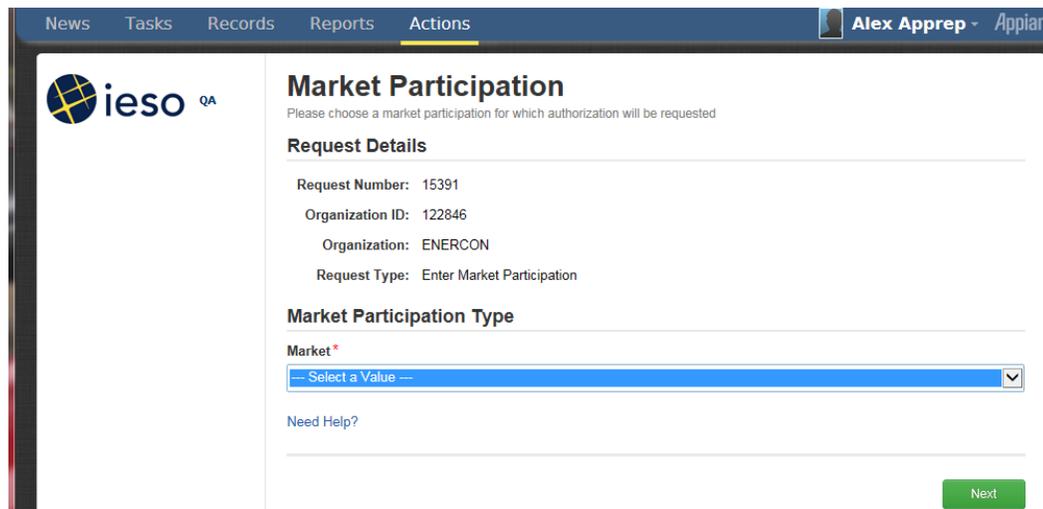
Figure 8-4: Online IESO Applicant Representative – Select Participation Type Page

The Applicant Representative can choose one of 3 options from the drop down and click on the 'Next' button. This will limit choosing the actual type of participation.



**Figure 8-5: Online IESO Applicant Representative – Select Participation Type Option**

For example, if Market Participation is chosen then the Applicant Representative will be present with the page shown in figure 8-6.



**Figure 8-6: Online IESO Applicant Representative – Market Participation Type**

The Applicant Representative can then choose the desired participation for the Market category from the dropdown list as shown below



**Figure 8-7: Online IESO Applicant Representative – Market Participation Choices**

The Applicant Representative could choose for example to enable her/his organization in the Capacity Auction market as shown in Figure 8-8 and then click on the 'Next' button.

**Market Participation**

Please choose a market participation for which authorization will be requested

**Request Details**

Request Number: 19366  
 Organization ID:  
 Organization:  
 Request Type: Enter Market Participation

**Market Participation Type**

Market \*  
 Capacity Auction

Your organization is eligible to participate in the Capacity Auction.

[Need Help?](#)

**NEXT**

**Figure 8-8: Online IESO Applicant Representative – Choosing Capacity Auction Market Participation**

The page would then update to show the Applicant Representative what tasks are next needed to be done as shown in Figure 8-9

News Tasks (13) Records Reports **Actions**

Required Tasks to Complete

Listed below are the tasks that must be completed by the requesting organization for this participation type.

**Request Details**

Request Number: 19366  
 Organization ID:  
 Organization:  
 Request Type: Enter Market Participation  
 Participation Type: Capacity Auction

**Required Tasks**

Confirm Connectivity to IESO Information System(s)

Assign Contact Role(s)

[Need Help?](http://www.ieso.ca/registration.help/#2.4)

**Proceed** **Cancel**

**Figure 8-9: Online IESO Applicant Representative – Participation Required Tasks**

The Applicant Representative would just need to click on the ‘Proceed’ button to complete the Participation registration and continue back to the Actions main page and then assign contacts and verify connectivity for the contacts to the required IESO IT system that the participation is permitting.

### Update Organization and Contacts

The Applicant Representative can choose ‘Update Organization’ to update Contact Roles to add one or more people to a desired contact role once the required participations applied for have been granted and approved by the IESO. The list of contact roles available (dependent on the registered participations) is shown in Appendix B.

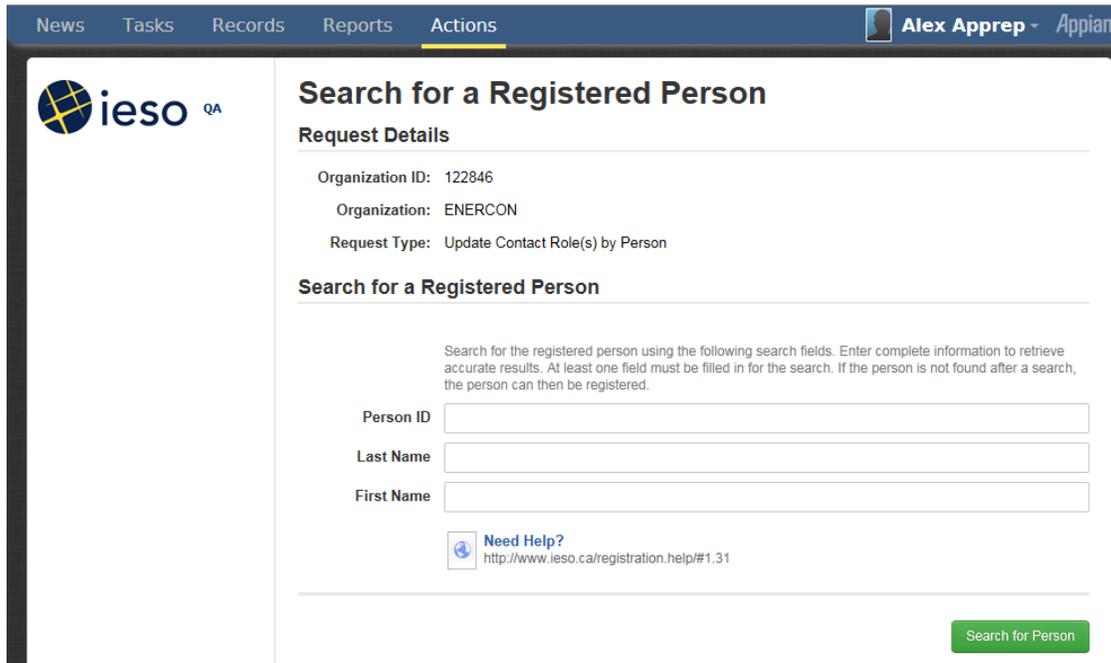
Once a required participation for an organization is active the Applicant Representative can choose Update Organization and then choose to Update Contact Role(s) from the dropdown list as shown in Figure 8-10 and then click on the Next button to proceed.

**Figure 8-10: Online IESO Applicant Representative Update Organization Request Type**

They can then choose to do so: “By Person”, “By Role” or “By Section” buttons

**Figure 8-11: Online IESO Applicant Representative Update Contact Role(s) Update Type**

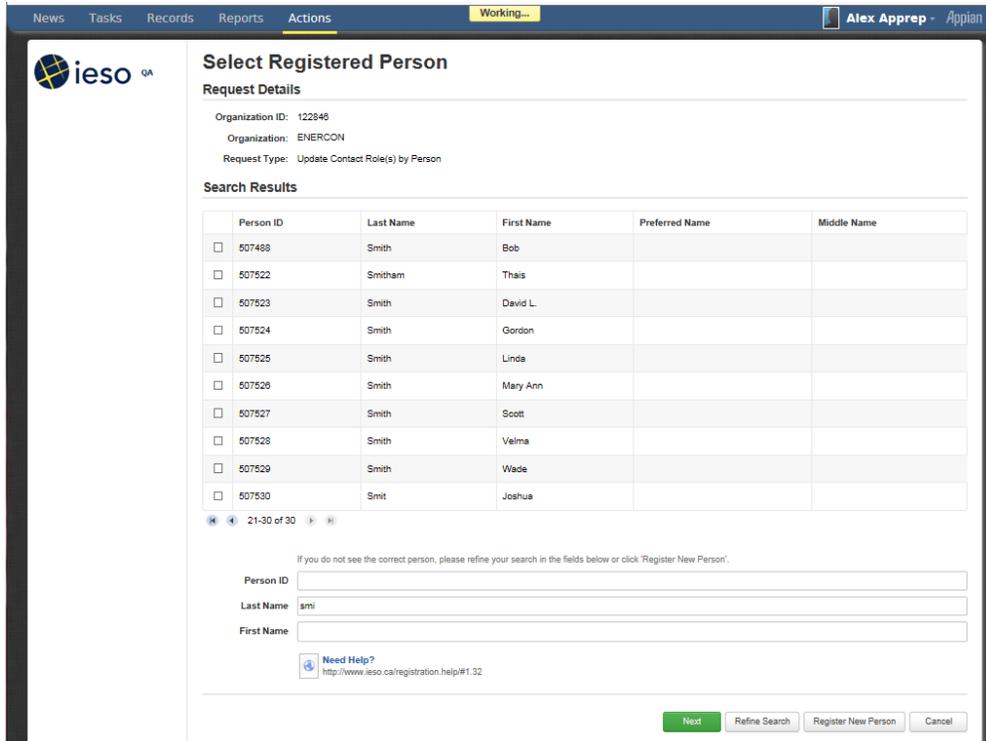
If choosing ‘By Person’ the Applicant Representative will need to know some information about the person, they want to register a contact role for so they can search for and choose that person.



The screenshot displays the IESO online registration system interface. At the top, there is a navigation bar with tabs for News, Tasks, Records, Reports, and Actions. The user's name, Alex Apprep, and the word Appian are visible in the top right corner. The main content area features the IESO logo on the left and a section titled "Search for a Registered Person". Below this title, the "Request Details" are shown: Organization ID: 122846, Organization: ENERCON, and Request Type: Update Contact Role(s) by Person. The search section includes a heading "Search for a Registered Person" and a paragraph of instructions: "Search for the registered person using the following search fields. Enter complete information to retrieve accurate results. At least one field must be filled in for the search. If the person is not found after a search, the person can then be registered." There are three input fields labeled "Person ID", "Last Name", and "First Name". Below these fields is a "Need Help?" link with the URL <http://www.ieso.ca/registration.help/#1.31>. A green "Search for Person" button is located at the bottom right of the search area.

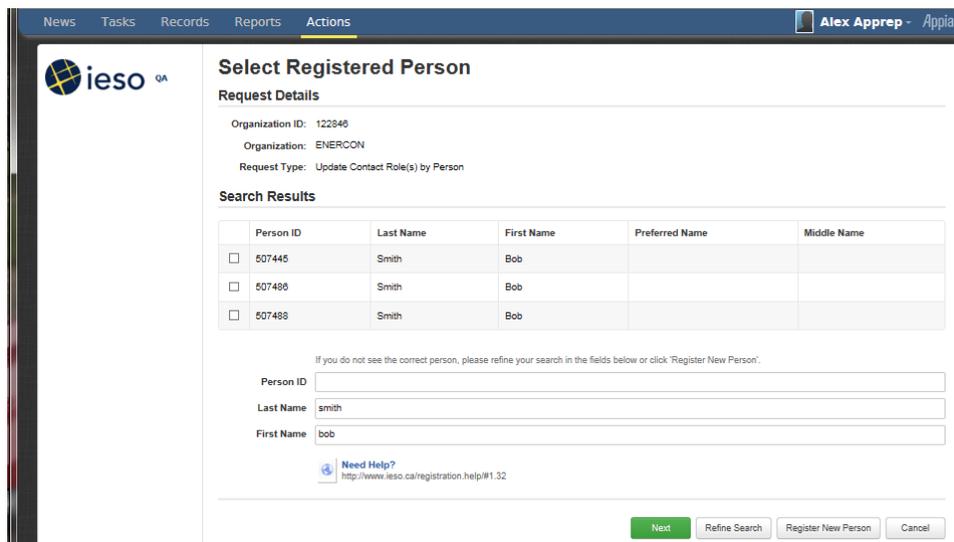
**Figure 8-12: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search**

For example, if the Applicant Representative knows the person's last name is Smith he/she can type Smith (or any part of the last name) in and click on 'Search for Person'. The results would show all people with Smith (or all those with last names matching the pattern input) as a last name and the Applicant Representative can sift through the list until they find the right person. The list is not necessarily sorted alphabetically so multiple pages may have to be looked at.



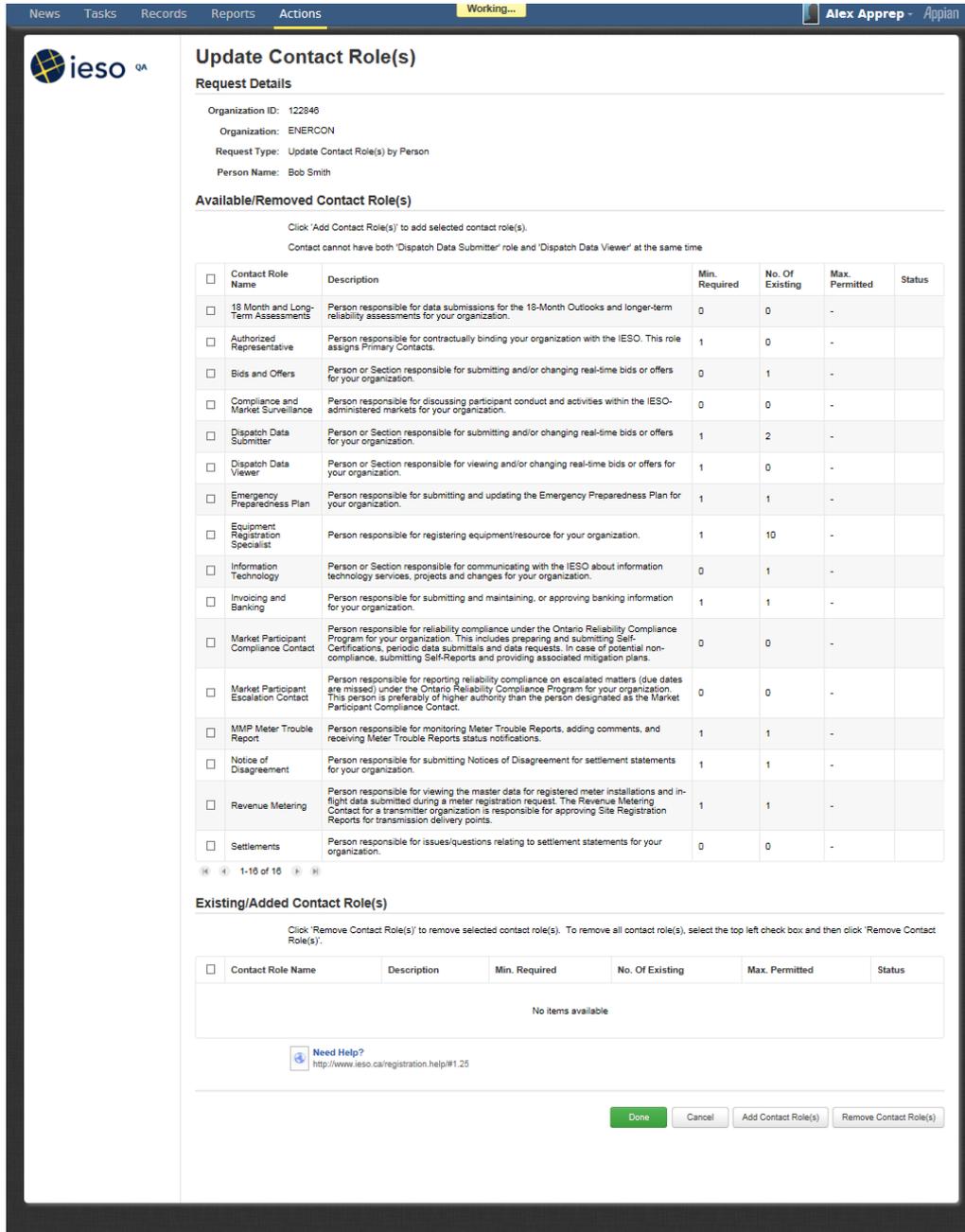
**Figure 8-13: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search Results**

The Applicant Representative can enter in both last and first names and do a search. For example, here is an example for “Smith” and “Bob”.



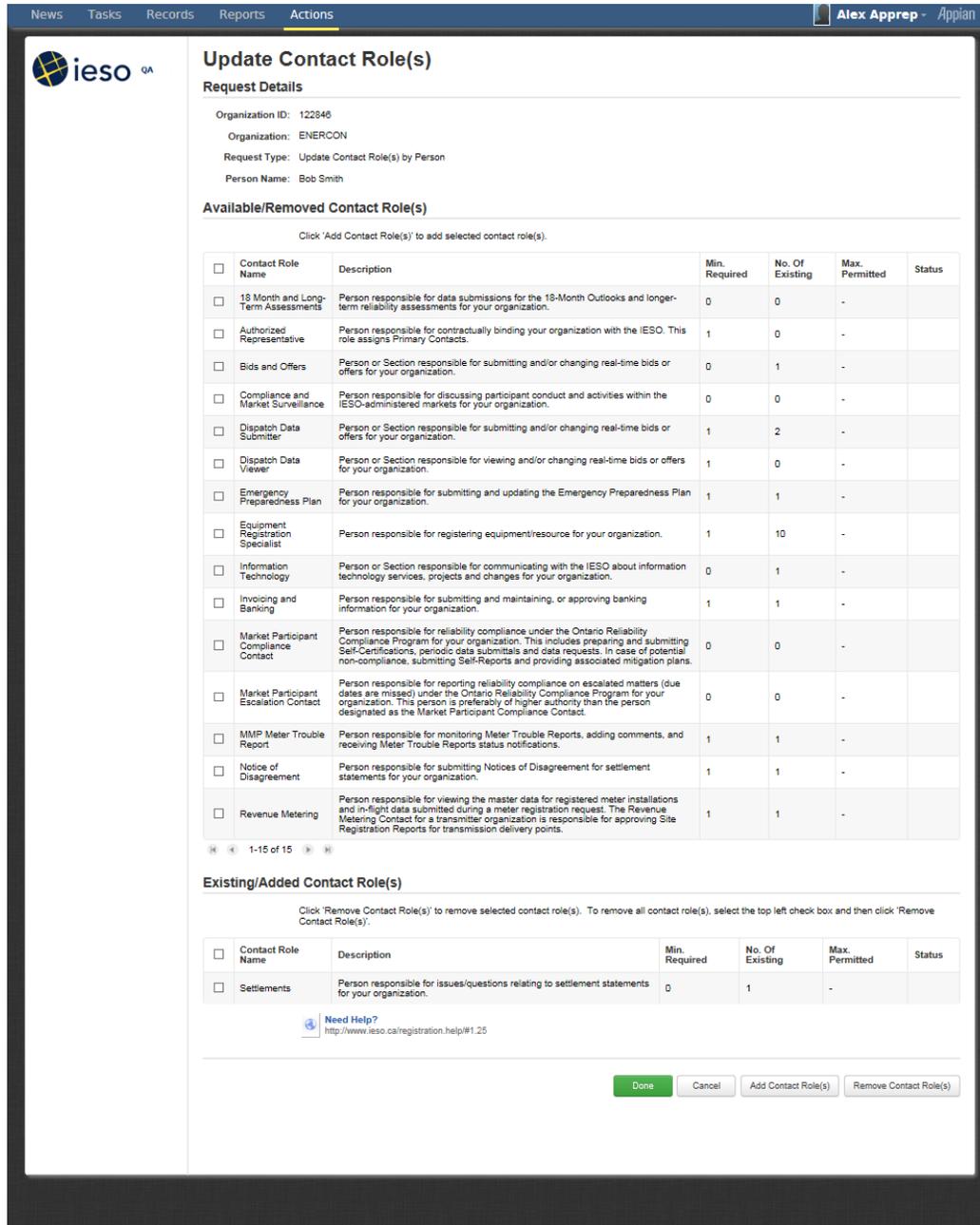
**Figure 8-14: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search Results 2**

The Applicant Representative upon finding and choosing the right person, for example “Bob Smith” with the correct Person ID, would check mark that person in the list and click on ‘Next’. The system will then present a list of available contact roles that person can be made a member of. The Applicant Representative must make absolutely sure they are choosing the correct person where multiple people have the same name.



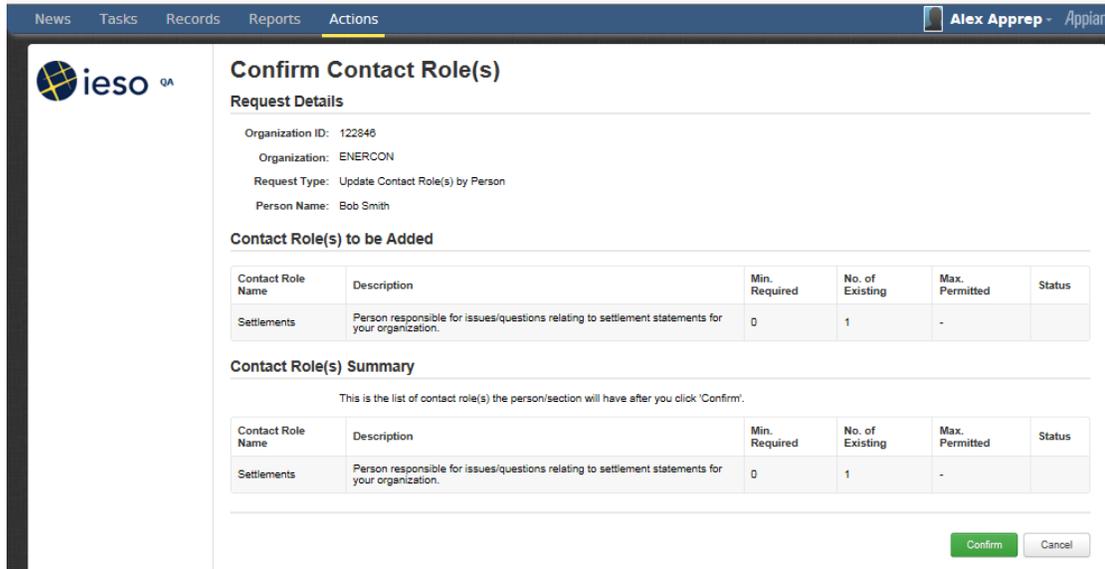
**Figure 8-15: Online IESO Applicant Representative Update Contact Role(s) Selection for Selected Person**

If the person needed to be added as a Settlements contact the Applicant Representative would check mark that Contact Role selection and click on the Add Contact Role(s) button. In this example the page will update showing that one person will now be added to the Settlements Contact Role



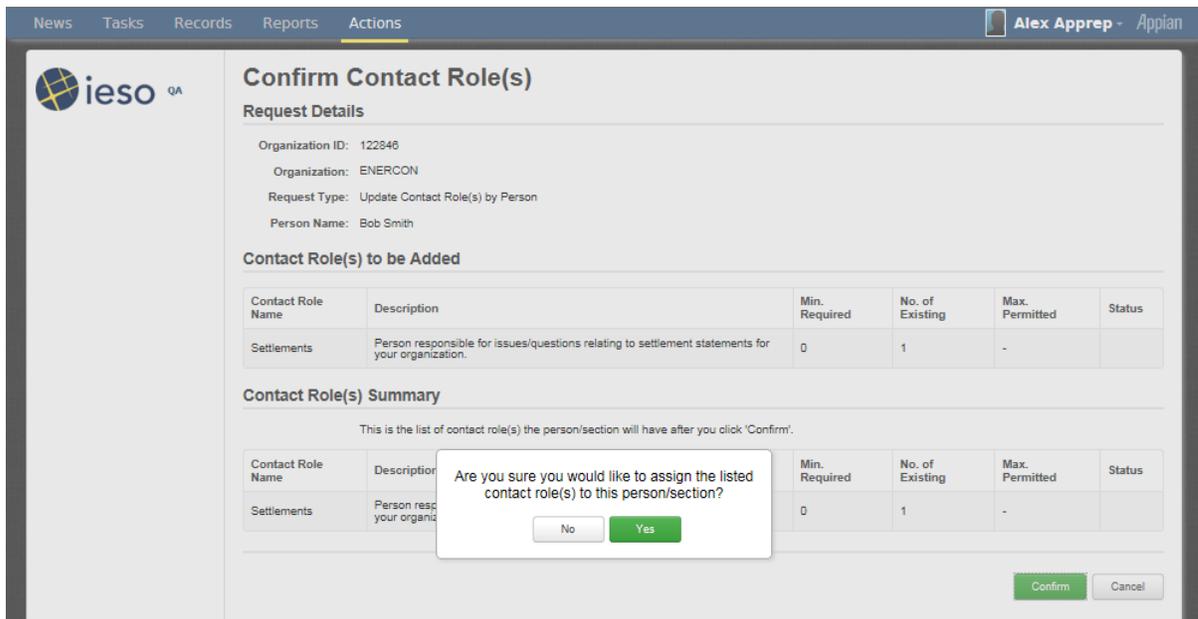
**Figure 8-16: Online IESO Applicant Representative Update Contact Role(s) Added Person**

The Applicant Representative will then click on the ‘Done’ button to continue with registering the person as a contact or ‘Cancel’ or choose and ‘Add (other) Contact Role(s)’ or choose and ‘Remove (other) Contact Role(s)’. Upon choosing ‘Done’ the page shown in Figure 8-17 will be displayed. Where applicable automated provisioning with the IESO Gateway system will add the person’s actual user account to the required role group(s) so that they have access ASAP.



**Figure 8-17: Online IESO Applicant Representative Update Contact Role(s), Confirmation**

The Applicant Representative can choose ‘Confirm’ or ‘Cancel’. Upon choosing confirm he/she will get one last chance to abort the addition or go ahead with it as shown in Figure 8-18.



**Figure 8-18: Online IESO Applicant Representative Update Contact Role(s), Final Confirmation**

Alternatively, the Applicant Representative can choose the ‘By Role’ selection to retrieve all applicable roles for their organization’s active participations. This will result in a list similar to the one shown in Figure 8-19.

**Select Contact Role**

**Request Details**

Organization ID: 122848  
 Organization: ENERCON  
 Request Type: Update Contact Role(s) by Role

**Available Contact Role(s)**

All of the contact role(s) listed below are contact role(s) that can be assigned based on your organization's existing participation(s). The table provides a description of each contact role, the minimum and maximum number of contacts permitted and the current number of contacts at your organization in each role. Please select the contact role you want to update and select next.

Contact Role Name	Description	Min. Required	No. of Existing	Max. Permitted
<input type="checkbox"/> 18 Month and Long-Term Assessments	Person responsible for data submissions for the 18-Month Outlooks and longer-term reliability assessments for your organization.	0	0	-
<input type="checkbox"/> Authorized Representative	Person responsible for contractually binding your organization with the IESO. This role assigns Primary Contacts.	1	0	-
<input type="checkbox"/> Bids and Offers	Person or Section responsible for submitting and/or changing real-time bids or offers for your organization.	0	1	-
<input type="checkbox"/> Compliance and Market Surveillance	Person responsible for discussing participant conduct and activities within the IESO-administered markets for your organization.	0	0	-
<input type="checkbox"/> Day-Ahead-Bids and Offers	Person or Section responsible for submitting and/or changing day-ahead bids or offers for your organization.	0	0	-
<input type="checkbox"/> Dispatch Data Submitter	Person or Section responsible for submitting and/or changing real-time bids or offers for your organization.	1	2	-
<input type="checkbox"/> Dispatch Data Viewer	Person or Section responsible for viewing and/or changing real-time bids or offers for your organization.	1	0	-
<input type="checkbox"/> Emergency Preparedness Plan	Person responsible for submitting and updating the Emergency Preparedness Plan for your organization.	1	1	-
<input type="checkbox"/> Equipment Outage Late Notification Contact	Person responsible for receiving email notification on outages that are late to start and taking appropriate actions.	0	1	-
<input type="checkbox"/> Equipment Outage Submitter	Person responsible for submitting, updating and canceling outage request on equipment owned or operated by your organization.	1	2	-
<input type="checkbox"/> Equipment Outage Viewer	Person who can view outage information on equipment owned or operated by your organization, and equipment permitted for viewing by other organizations.	0	1	-
<input type="checkbox"/> Equipment Registration Specialist	Person responsible for registering equipment/resource for your organization.	1	10	-
<input type="checkbox"/> Information Technology	Person or Section responsible for communicating with the IESO about information technology services, projects and changes for your organization.	0	1	-
<input type="checkbox"/> Invoicing and Banking	Person responsible for submitting and maintaining, or approving banking information for your organization.	1	1	-
<input type="checkbox"/> Market Participant Compliance Contact	Person responsible for reliability compliance under the Ontario Reliability Compliance Program for your organization. This includes preparing and submitting Self-Certifications, periodic data submissions and data requests, in case of potential non-compliance, submitting Self-Reports and providing associated mitigation plans.	0	0	-
<input type="checkbox"/> Market Participant Escalation Contact	Person responsible for reporting reliability compliance on escalated matters (due dates are missed) under the Ontario Reliability Compliance Program for your organization. This person is preferably of higher authority than the person designated as the Market Participant Compliance Contact.	0	0	-
<input type="checkbox"/> MMP Meter Trouble Report	Person responsible for monitoring Meter Trouble Reports, adding comments, and receiving Meter Trouble Reports status notifications.	1	1	-
<input type="checkbox"/> Notice of Disagreement	Person responsible for submitting Notices of Disagreement for settlement statements for your organization.	1	1	-
<input type="checkbox"/> Prudential Requirements	Person responsible for submitting prudential information and is the point of contact for any issues regarding prudentials (margin calls, warnings and defaults) for your organization.	1	0	-
<input type="checkbox"/> Revenue Metering	Person responsible for viewing the master data for registered meter installations and in-flight data submitted during a meter registration request. The Revenue Metering Contact for a transmitter organization is responsible for approving Site Registration Reports for transmission delivery points.	1	1	-
<input type="checkbox"/> Revenue Metering Data	Person responsible for managing meter data report profiles, as well as requesting and retrieving revenue meter data reports for your organization.	1	1	-
<input type="checkbox"/> Settlements	Person responsible for issues/questions relating to settlement statements for your organization.	0	0	-

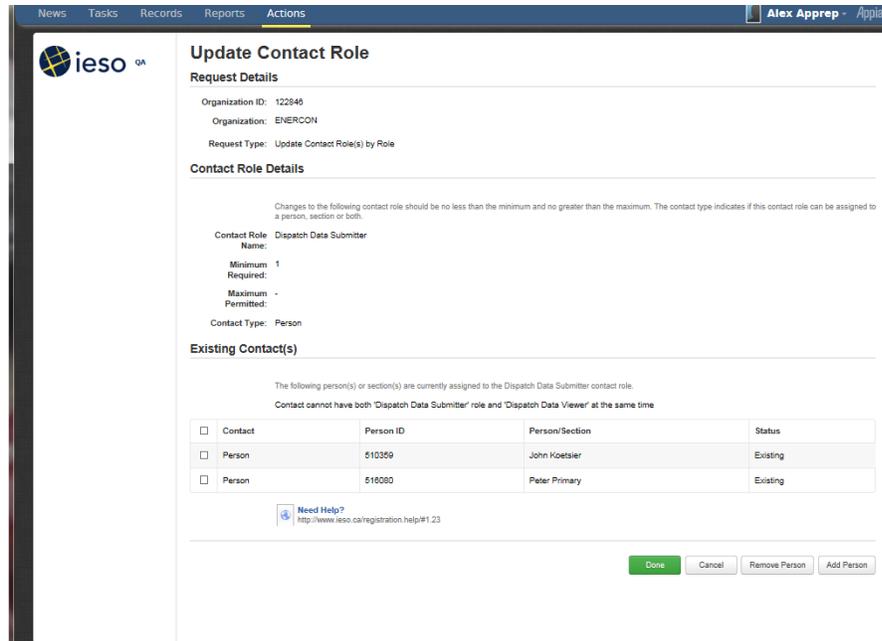
1-22 of 22

[Need Help?](http://www.ieso.ca/registration/help/122)  
<http://www.ieso.ca/registration/help/122>

Next Cancel

**Figure 8-19: Online IESO Applicant Representative Update Contact Role(s) Select Contact Role List**

Choosing any contact role – for example, Dispatch Data Submitter and clicking on the Next button will show a list of those already in that role (Figure 8-20) and options to Cancel, Remove Person or Add Person or choose ‘Done’. Choosing Add Person will provide the ‘Search for a Registered Person’ page as shown above in Figure 8-6.



**Figure 8-20: Online IESO Applicant Representative Update Contact Role(s) – Existing Contacts**

Choosing the desired “Bob Smith” person and the Next button will result in that shown in Figure 8-21. The existing people will show as existing and “Bob Smith” with no status.

**Update Contact Role**

**Request Details**

Organization ID: 122846  
 Organization: ENERCON  
 Request Type: Update Contact Role(s) by Role

**Contact Role Details**

Changes to the following contact role should be no less than the minimum and no greater than the maximum. The contact type indicates if this contact role can be assigned to a person, section or both.

Contact Role Name: Dispatch Data Submitter  
 Minimum Required: 1  
 Maximum Permitted: -  
 Contact Type: Person

**Existing Contact(s)**

The following person(s) or section(s) are currently assigned to the Dispatch Data Submitter contact role.  
 Contact cannot have both 'Dispatch Data Submitter' role and 'Dispatch Data Viewer' at the same time

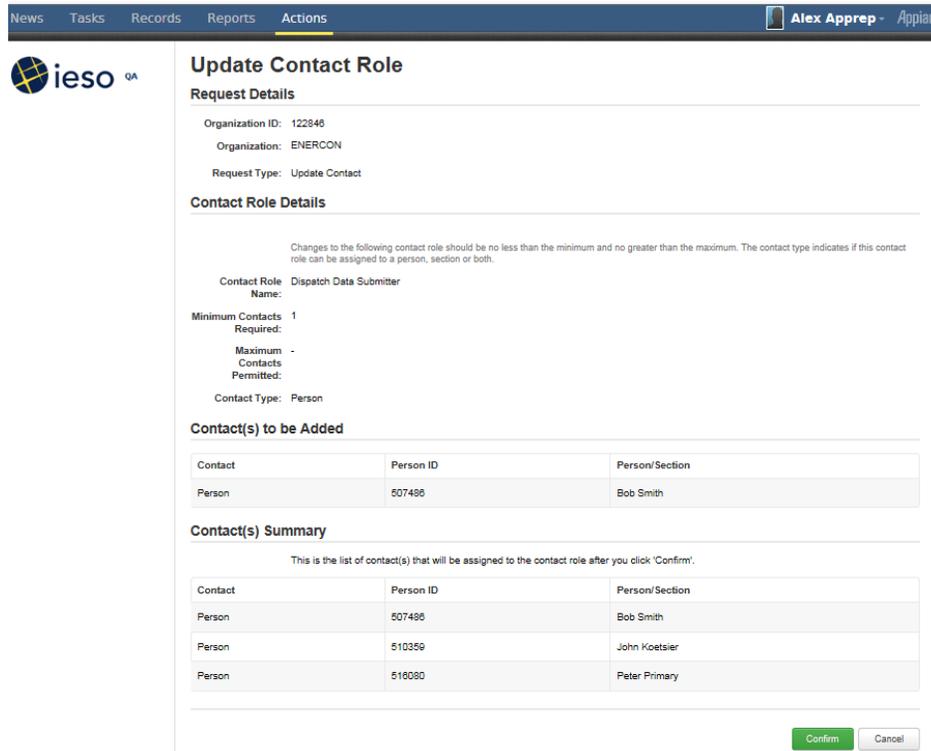
<input type="checkbox"/>	Contact	Person ID	Person/Section	Status
<input type="checkbox"/>	Person	507498	Bob Smith	
<input type="checkbox"/>	Person	510359	John Koetsier	Existing
<input type="checkbox"/>	Person	518080	Peter Primary	Existing

[Need Help?](http://www.ieso.ca/registration.help/#1.23)

Done Cancel Remove Person Add Person

**Figure 8-21: Online IESO Applicant Representative Update Contact Role(s) – Existing plus New Contacts**

Clicking on done will display a primary Confirmation page as in Figure 8-22. Clicking on Confirm will prompt the Applicant Representative to choose Yes or No to proceed. Choosing ‘Yes’ will add the person to the contact role. Where applicable automated provisioning with the IESO Gateway system will update the person’s actual user account to the additional required role group(s) so that their access is updated ASAP.



**Figure 8-22: Online IESO Applicant Representative Update Contact Role(s) – Primary Confirmation**

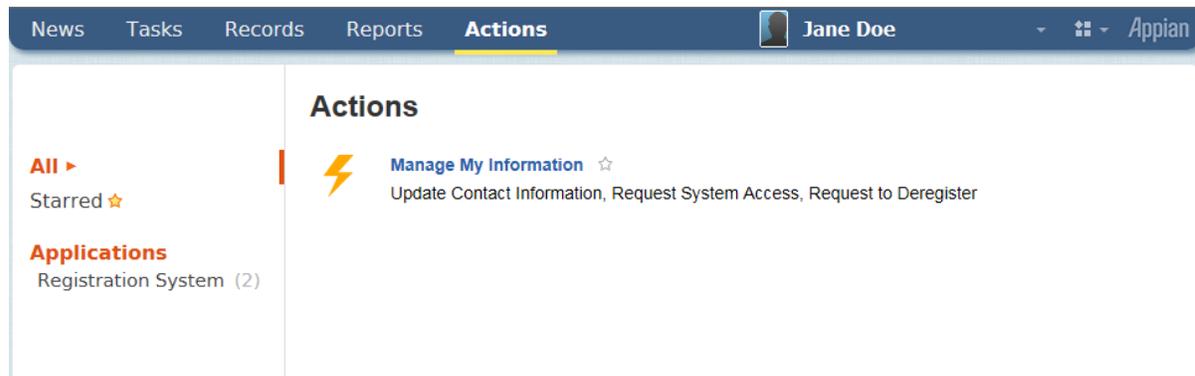
**Rights Administrator**

Successful login to the Online IESO Registration system by a Rights Administrator will take them to an Actions page as shown in Figure 8-23. The Rights Administrator user can choose “Grant/Revoke Access” to begin a process instance for granting or revoking IESO systems access for a User Account for the *participant(s)* the Rights Administrator represents. He or she can also choose to update their own personal contact information, request systems access to IESO systems (inside or outside of Online IESO) for themselves or request to register with the “Manage My Information” choice.



**Figure 8-23: Online IESO Registration System Rights Administrator Actions Page**

Other *participant* contacts can login to the Online IESO / Registration System and choose the “Manage My Information” task as shown by the example in Figure 8-24 to edit/update their own person information such as name, phone numbers, address, email addresses and any contact notes.

**Figure 8-24: Online IESO Registration System Normal Contact Actions Page**

### 8.1.3 Online IESO Registration System Grant/Revoke Access

#### Select System Access Request Type

Upon choosing the Grant/Revoke Access, task the Rights Administrator, if they only represent one *participant* organization, will be navigated to a “Select System Access Request Type” page as shown by the example in Figure 8-26 where the *participant* organization they represent will be shown and a drop down selection list of the System Access Request Types can be chosen to start the process.

If the Rights Administrator represents multiple *participant* organizations, they will first be navigated to a page “Choose an Organization” as shown by the example in Figure 8-25 where they must choose which organization they will be processing the Grant/Revoke access task for and click on the “Next” button.

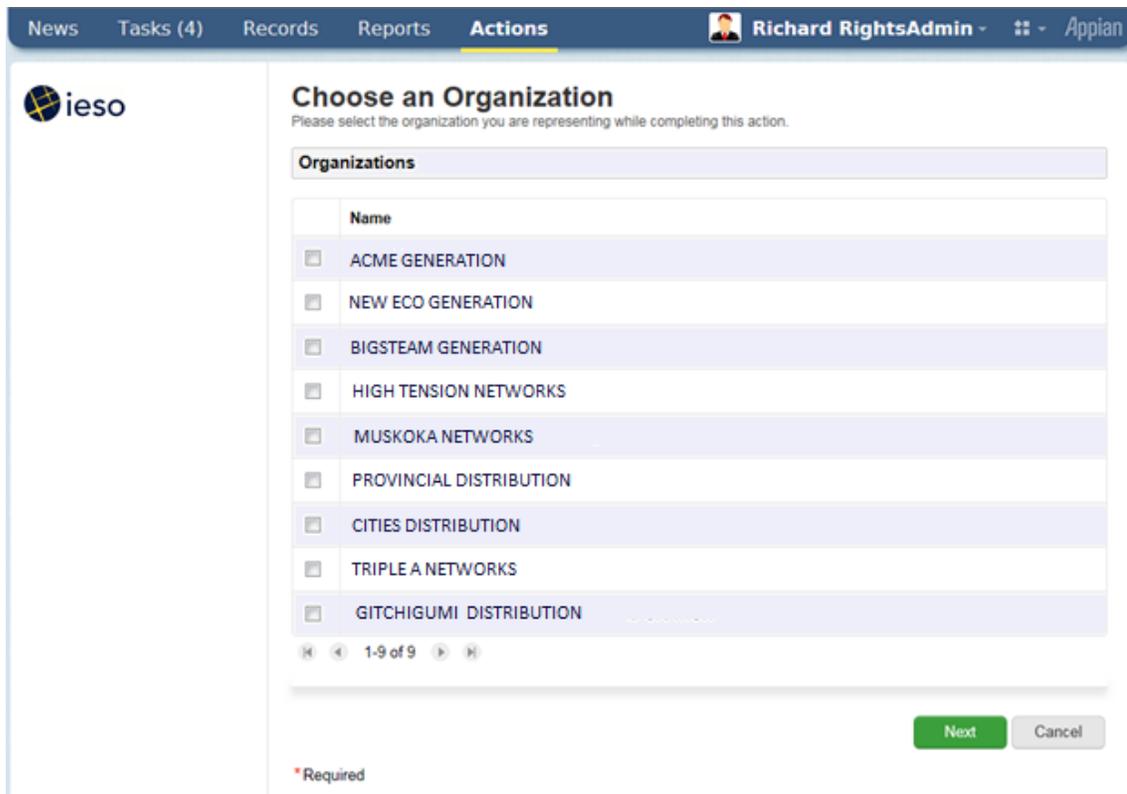
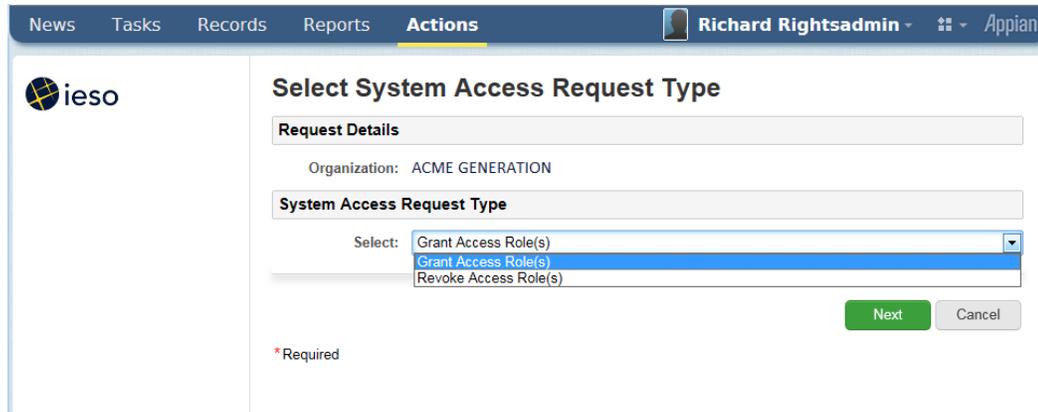


Figure 8-25: Choose an Organization Page

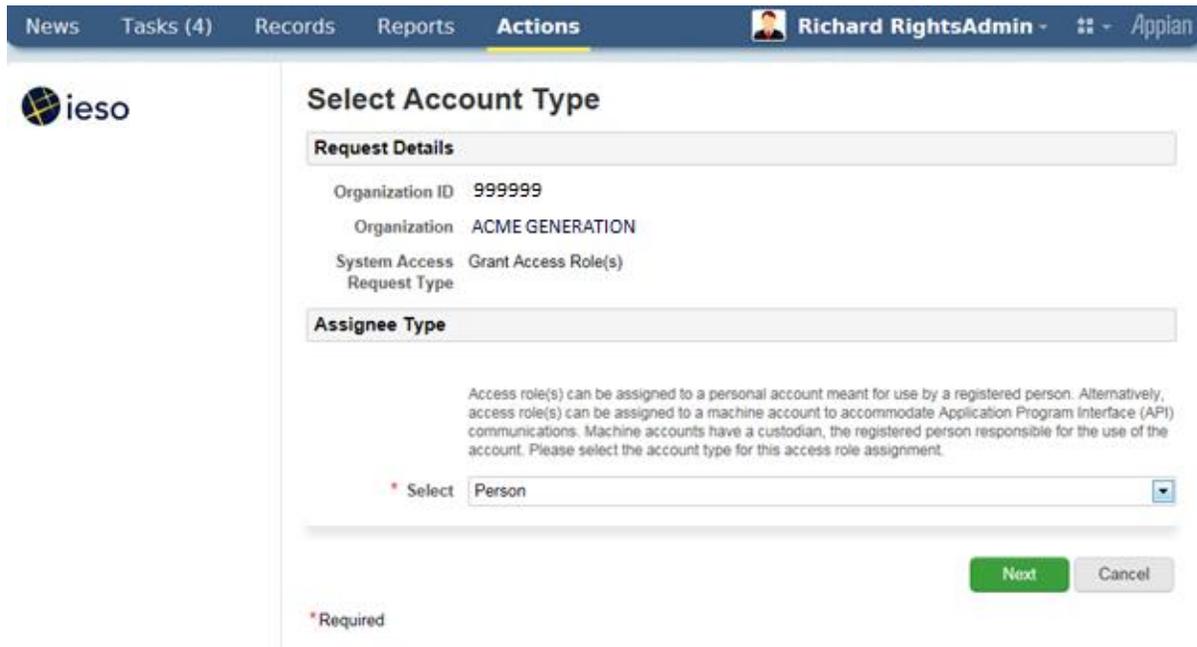


**Figure 8-26: Select System Access Request Type Page**

Upon landing on the Select System Access Request Type Page the Rights Administrator must choose either “Grant Access Role(s)” or “Revoke Access Role(s)” as required by the situation and click on the “Next” button. This will navigate the Rights Administrator to a “Select Account Type” page as shown in Figure 8-27. In the example provided, a grant access role(s) request is shown. The page for revoke access role(s) will be similar.

Both the “Grant Access Role(s)” or “Revoke Access Role(s)” processes will require the selection of an account type. However, while the “Grant Access Role(s)” process will later let the Rights Administrator choose an existing person or machine account or create a new person or machine account, the “Revoke Access Role(s)” will only apply to existing person or machine accounts.

**Select Account Type**



**Figure 8-27: Select Account Type Page - Grant**

The choices in the drop down list for account type are “Person” for use by an individual or “Machine” for use with API communications. The Rights Administrator must choose one or the other as the situation requires and click on the “Next” button to continue. This will navigate the Rights Administrator to a “Search for a Registered Person” page as shown in Figure 8-28 where they can search for the person who already possesses a user account. In the example provided, a grant access role(s) request page is shown. The page for revoke access role(s) will be similar for selecting a registered person.

## Search and Select a Registered Person

The screenshot shows the IESO web interface. At the top, there is a navigation bar with tabs for News, Tasks (4), Records, Reports, and Actions. The user is logged in as Richard RightsAdmin. The main content area is titled "Search for a Registered Person". Under "Request Details", the following information is displayed: Organization ID 999999, Organization ACME GENERATION, System Access Grant Access Role(s), Request Type, and Account Type Person. Below this is a section for searching for a registered person, which includes a text box with instructions: "Search for the registered person using the following search fields. Enter complete information to retrieve accurate results. At least one field must be filled in for the search. If the person is not found after a search, the person can then be registered." There are three input fields for Person ID, Last Name, and First Name. At the bottom right, there are two buttons: "Search for Person" (green) and "Cancel" (grey). A red asterisk indicates that the Person ID field is required.

**Figure 8-28: Search for a Registered Person Page - Grant**

The Rights Administrator can search based on the Person ID if it is known (i.e. it should be) or the last name or first name of the person that the Grant/Revoke access role(s) request is for. Once the Rights Administrator has filled in the search parameters he or she must click on the “Next” button. This will start the search and return all existing results as shown by the example for “Select a Registered Person” page in Figure 8-29 or none if there is no match found.

It is possible that person record(s) may be retrieved for people with the same first and last names as the actual person the Rights Administrator is dealing with. It is up to the Rights Administrator to verify that an existing person record retrieved is for the intended person or not. For grant access role(s) requests, if no existing registered person record exists for the intended person, the Rights Administrator can proceed to creation of a new person record for the targeted individual. The Rights Administrator should conduct a thorough search via the “Refine Search” button before selecting one of the retrieved person results and clicking on the “Next” button before attempting to create a new Person Record with the Register New Person.

Note that for all existing registered persons, User Accounts will already exist for them.

For Persons being newly registered by the Rights Administrator for the grant access role(s) request process, the Registration system will at the appropriate point in the process include within the automated provisioning grant request issued to the IESO Gateway system, the instructions to create an account for the person with an automatically assigned User Name. Once IESO Gateways system creates the actual account, the system will send an activation email the person with the user account details.

**Select Registered Person**

**Request Details**

Organization ID 999999  
 Organization ACME GENERATION  
 System Access Grant Access Role(s)  
 Request Type  
 Account Type Person

**Search Results**

The search returned the following registered persons. Select the registered person you were searching. If the results did not retrieve the person, refine your search or select Register New Person.

	Person ID	Last Name	First Name	Preferred Name	Middle Name
<input checked="" type="checkbox"/>	507433	Somer	Em		

1-1 of 1

If the results did not retrieve the person you were searching, try again by modifying the search fields below.

Person ID   
 Last Name   
 First Name

\* Required

**Figure 8-29: Select a Registered Person Page - Grant**

Where an existing person record is not found and the Rights Administrator clicks on the “Register New Person” button, the Rights Administrator will be navigated to a “Register a New Person” page as shown by the example in Figure 8-30.

If the Rights Administrator does choose an existing person by check marking the row and clicking on the Next button he or she will be navigated to:

- A “Select Access Roles to be Granted” page as shown in Figure 8-32 if the “Grant Access Role(s)” system access request type was chosen or
- A “Select Access Roles to be Revoked” page as shown in Figure 8-34 if the “Revoke Access Role(s)” system access request type was chosen.

## Register a New Person

The screenshot shows the 'Register a New Person' page in the IESO system. At the top, there is a navigation bar with 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions' (highlighted). The user is identified as 'Richard RightsAdmin' with an 'Appian' logo. The IESO logo is on the left. The main heading is 'Register a New Person'. Below it is a 'Request Details' section with the following information:

- Organization ID: 999999
- Organization: ACME GENERATION
- System Access Request Type: Grant Access Role(s)
- Account Type: Person

A note states: 'Please fill in the mandatory information below. The address fields have been populated with the organization's registered address but can be modified. Please note an email will be sent to this person upon registration.'

The 'Person Information' section contains the following fields:

- \* First Name (required)
- \* Last Name (required)
- \* Main Phone (required) with an example: 123-456-7890
- Main Phone Extension (optional) with a note: Numbers only
- \* Main Email (required)
- \* Address Line 1 (required)
- Address Line 2 (optional)
- Address Line 3 (optional)
- Address Line 4 (optional)
- \* City (required)
- \* Province/State (required) with a dropdown menu showing 'N/A' and a note: 'Outside Canada or USA, select N/A'
- \* Postal Code/Zip Code (required) with an example: 'R3T 2T5 or 12345, if unknown, use N/A'
- \* Country (required) with a dropdown menu showing 'Canada'

A green 'Next' button is located at the bottom right. A legend at the bottom left indicates that an asterisk (\*) denotes a required field.

**Figure 8-30: Register a New Person Page - Grant**

All required attributes for the person must be filled in before clicking on “Next” button. A new unique Person ID will be automatically assigned by the system when it is saved and this can be referenced later as required.

When the Rights Administrator clicks on “Next” he or she will be navigated to a Confirm New Person Registration as shown in Figure 8-31. The Rights Administrator can choose to “Go Back” to correct or fill in any information or click on the “Next” button.

The screenshot shows the 'Confirm New Person Registration' page. At the top, there is a navigation bar with 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions'. The user is logged in as 'Richard RightsAdmin'. The page title is 'Confirm New Person Registration' with a sub-note: 'Click "next" to register the person, an email will then be sent to the person. Ensure you have entered the information correctly as it may be used to send confidential information.'

The page is divided into two main sections:

- Request Details:**
  - Organization ID: 999999
  - Organization: ACME GENERATION
  - System Access Request Type: Grant Access Role(s)
  - Account Type: Person
- Person Information:**
  - First Name: Jane
  - Last Name: Doe
  - Main Phone: 123-456-7890
  - Main Email: test@test.com
  - Address Line 1: 12 Park Lane
  - Address Line 2:
  - Address Line 3:
  - Address Line 4:
  - City: Greenville
  - Province/State: Ontario
  - Postal Code/Zip Code: 1Q2 W3E
  - Country: Canada

At the bottom, there are three buttons: 'Go Back', 'Next' (highlighted in green), and 'Cancel'. A red asterisk indicates required fields.

**Figure 8-31: Confirm New Person Registration Page - Grant**

After the Register and Confirm New Person Registration sub-process flow the Rights Administrator will then be navigated to the “Select Access Roles to be Granted” page as shown in Figure 8-32. Note that the Person ID information is now displayed.

In the case of revoking access roles, the Rights Administrator will then be navigated to the “Select Access Roles to be Revoked” page as shown in Figure 8-34.

The information displayed for an existing person being processed for either a grant or revoke access role(s) request will show any existing access roles (that a user account for the person is associated with) for the *participant* organization.

The “Select Access Role(s) to be Granted” page will only display personal account related access roles associated to the Market or Program participation that the organization has registered for. This is true for the “Select Access Role(s) to be Revoked” page as well.

This is to prevent unintended automated provisioning Grant or Revoke requests from being submitted to the IESO Gateway system for the *participant* person. If an access role is not shown that the Rights Administrator thinks should be there, he or she should contact IESO Customer Relations. It is possible that a technical problem could exist or it may be possible that the *participant* needs to register for additional Markets or Programs. This document does not cover registering for Markets or Programs by a *participant*.

### Select Access Roles to be Granted

**Request Details**

Organization ID 999999  
Organization ACME GENERATION  
System Access Grant Access Role(s)  
Request Type  
Account Type  
Person Jane Doe  
Person ID 507435

**Existing Access Role(s)**

Role Name	Description
No items available	

1-1 of 0

**Access Roles**

Select Access Role(s) to assign. The access role(s) listed correspond to the access role(s) that may be needed based on the organization's participation.

**Financial Market Operations/Settlements**

<input type="checkbox"/>	Role Name	Description
<input type="checkbox"/>	Financial Market Trading & Reports	Submit Transmission Rights Auction bids via the Transmission Rights Auction application. Retrieve financial market reports via the IESO Participant Reports site.
<input type="checkbox"/>	Financial Market Reports	Retrieve financial market reports via the IESO Participant Reports site.

1-2 of 2

**Participation Settlements**

<input type="checkbox"/>	Role Name	Description
<input type="checkbox"/>	Settlements Submission & Settlements Reports	Submit & search settlement information via the Online Settlement Request Form system. Retrieve settlement reports via the IESO Participant Reports site.
<input type="checkbox"/>	Settlements Search & Settlements Reports	Search settlement information via the Online Settlement Request Form system. Retrieve settlement reports via the IESO Participant Reports site.
<input type="checkbox"/>	Notice Of Disagreement Submission	Submit notices of disagreement via the Workflow Notice of Disagreement system.
<input type="checkbox"/>	Settlements Reports	Retrieve settlement reports via the IESO Participant Reports site.

1-4 of 4

Next Cancel

\* Required

Figure 8-32: Select Access Roles to be Granted Page

The Rights Administrator should in the case of granting access roles to the person, choose only the required access roles (i.e. those authorized for the person by the *participant*) by check marking them

and clicking on the “Next” button. Multiple access roles available may be displayed by the first, next previous and last arrow buttons shown on the page.

Once the Rights Administrator has clicked on the “Next” button she or he will be navigated to a “Confirm Access Role(s) to be Granted” page as shown in Figure 8-33

**Confirm Access Role(s) to be Granted**  
Please confirm the access that will be granted to this person or machine account with this request.

**Request Details**

Organization ID 999999  
 Organization Name ACME GENERATION  
 System Access Grant Access Role(s)  
 Request Type  
 Account Type  
 Person Jane Doe  
 Person ID 507435

**Access Role(s) to be Granted**

Access Roles to Confirm for Account

Role Name	Description
Financial Market Trading & Reports	Submit Transmission Rights Auction bids via the Transmission Rights Auction application. Retrieve financial market reports via the IESO Participant Reports site.
Financial Market Reports	Retrieve financial market reports via the IESO Participant Reports site.

1-2 of 2

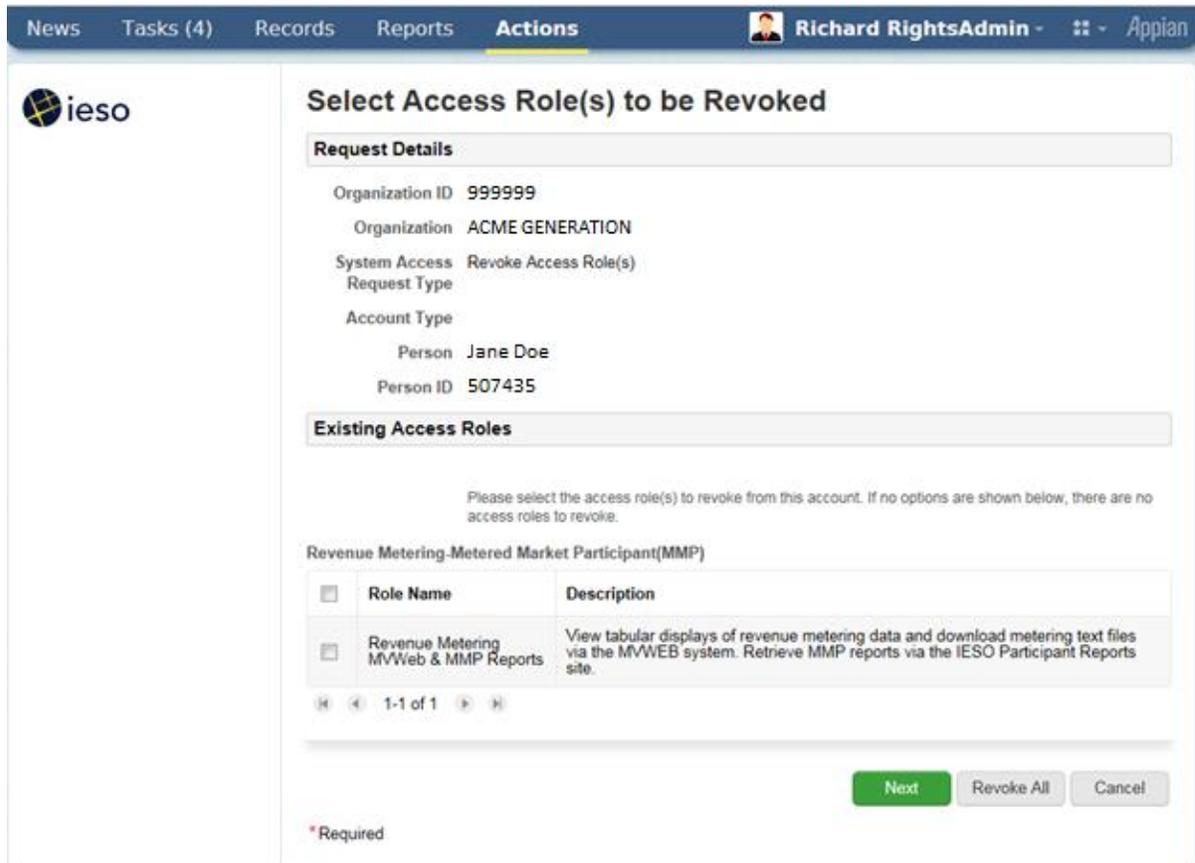
Go Back Confirm Cancel

\* Required

**Figure 8-33: Confirm Access Role(s) to be Granted Page**

The page will show the access roles selected and the Rights Administrator can use either the “Go Back” button to correct the selected access roles or click on the “Confirm” button and continue the process. Once confirmed the system will associate the access roles to the person’s primary user account for the *participant* organization chosen and send an automated provisioning grant request to the IESO Gateway system to enroll the person’s account in the access roles requested.

### Select Access Roles to be Revoked

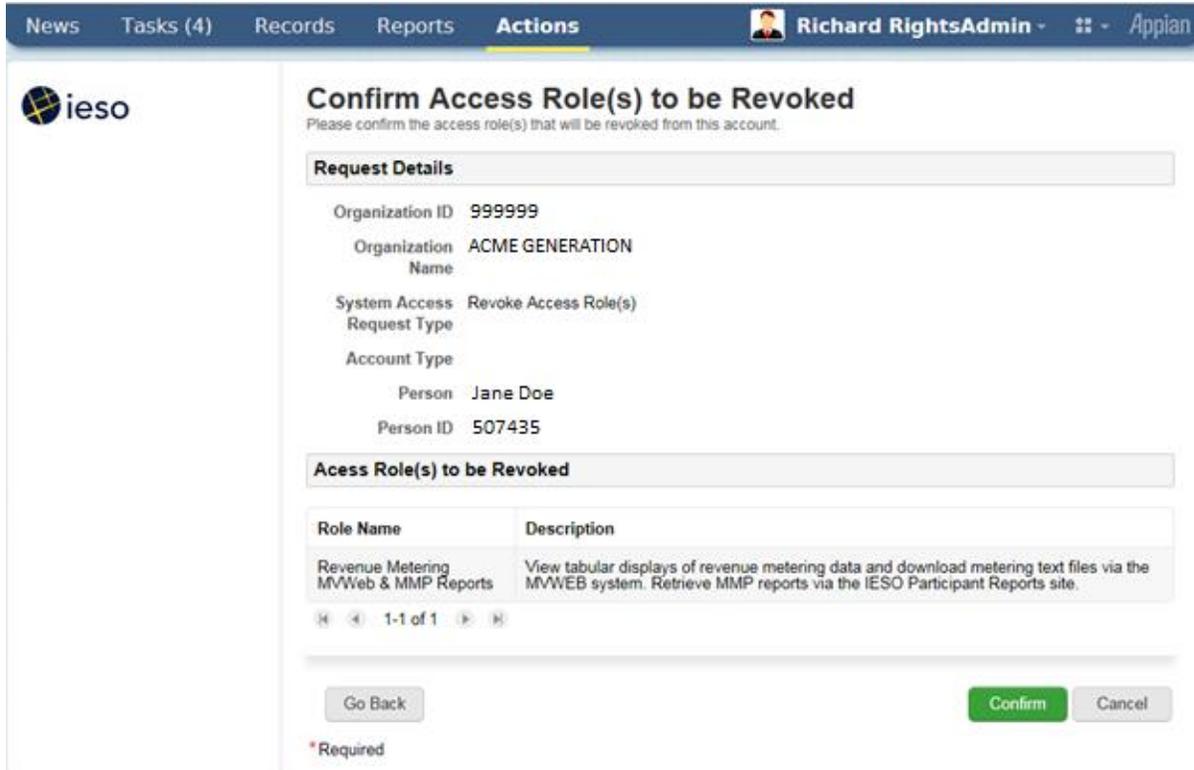


**Figure 8-34: Select Access Roles to be Revoked Page**

The “Select Access Role(s) to be Revoked” page will show only those access roles the person’s user account is currently associated with.

The Rights Administrator should in the case of revoking access roles to the person, choose only the targeted access roles (i.e. those authorized for revocation by the *participant*) by check marking them and clicking on the “Next” button. Multiple access roles available may be displayed by the first, next previous and last arrow buttons shown on the page. The page does provide a “Revoke All” button to conveniently permit the Rights Administrator to request revocation of all access roles for the person’s user account if that is what the Rights Administrator has been authorized to do.

Once the Rights Administrator has clicked on the “Next” button she or he will be navigated to a “Confirm Access Role(s) to be Revoked” page as shown in Figure 8-35



**Figure 8-35: Confirm Access Role(s) to be Revoked Page**

The page will show the access roles selected for revocation and the Rights Administrator can use either the “Go Back” button to correct the selected access roles or click on the “Confirm” button and continue the process. Once confirmed the system will process the access roles to be revoked for the person’s primary user account for the *participant* organization chosen and send an automated provisioning revoke request to the IESO Gateway system to remove the membership that the person’s user account has with the access roles requested.

## Machine Account Grant or Revoke Access Requests

When a Rights Administrator chooses the machine account selection within the dropdown on the “Select Account Type” page shown above in Figure 8-27 and clicks on the “next” button, she or he will be redirected to the “Select Machine Account” page as shown by the example in Figure 8-36 for grant access role(s) requests. The page for revoke access role(s) for machine account selection is shown by the example in Figure 8-37.

The Rights Administrator can choose to search for an existing machine account and choose it or click on the “New Machine Account” button if a new one is required. The Rights Administrator must know the Machine Account ID when he or she wants to find and choose an existing one and the choice of an existing one must be done carefully to prevent unintended access role changes and potential confidentiality breaches or loss of access.

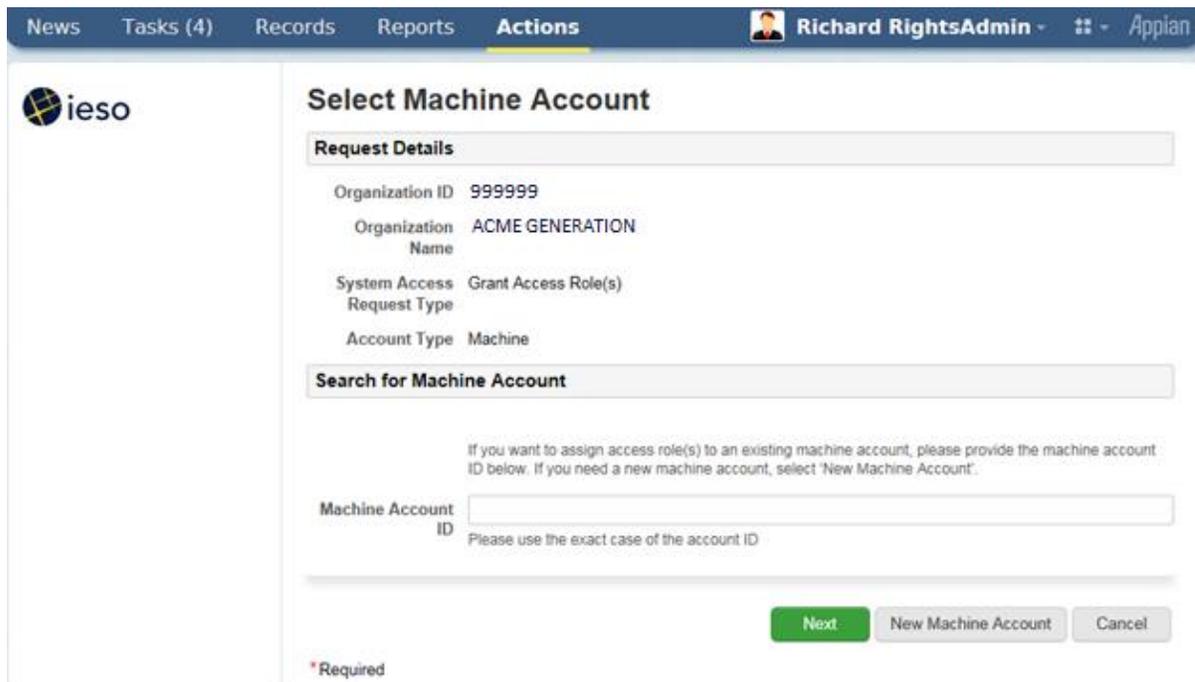


Figure 8-36: Select Machine Account Page - Grant

The screenshot displays the 'Select Machine Account' page within the IESO system. The top navigation bar includes 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions', with the user 'Richard RightsAdmin' logged in. The page header shows the IESO logo and the title 'Select Machine Account'. Under 'Request Details', the following information is shown: Organization ID 999999, Organization Name ACME GENERATION, System Access Request Type Revoke Access Role(s), and Account Type Machine. A 'Search for Machine Account' section contains a text input field for the Machine Account ID, with instructions to enter the exact case of the account ID. A warning message states: 'Warning: If your organization requires continued use of access role(s) that you are about to revoke, ensure that you already have another machine account with the required access role(s). By revoking access role(s) that are still needed, your organization may not be capable of conducting business with the IESO.' At the bottom, there are 'Go Back', 'Next', and 'Cancel' buttons, and a '\* Required' indicator.

**Figure 8-37: Select Machine Account Page - Revoke**

Note the warning regarding revocation of machine account access roles on the page.

If the Rights Administrator enters a non-existent Machine Account ID it will not be found and the system will inform the Rights Administrator when he or she clicks on the “Next” button.

If a machine account ID is found when the “Next” button is clicked, a “Confirm Existing Machine Account” page will be displayed as shown in the example in Figure 8-38. The page shown is for grant access role(s). The one for the revoke access roles for machine account process is similar.

The screenshot shows a web application interface for the IESO system. At the top, there is a navigation bar with tabs for 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions'. The user is logged in as 'Richard RightsAdmin' using 'Appian'. The main content area is titled 'Confirm Existing Machine Account'. It is divided into two sections: 'Request Details' and 'Machine Account Details'. The 'Request Details' section shows: Organization ID: 999999, Organization Name: ACME GENERATION, System Access Request Type: Grant Access Role(s), and Account Type: Machine. The 'Machine Account Details' section includes a note: 'The machine account ID provided has the following custodian. Select 'Next' if this is the right custodian to assign access role(s) to the account. If the custodian listed below is not right, select 'Go Back' to search again.' Below this, the details are: Machine Account ID: APIIESO00002, Person ID: 507370, First Name: F. Allen, and Last Name: Wiley. At the bottom, there are three buttons: 'Go Back', 'Next', and 'Cancel'. A small asterisk and the word 'Required' are visible at the bottom left.

**Figure 8-38: Confirm Existing Machine Account Page - Grant**

The “Confirm Existing Machine Account” page will show the selected machine account and its custodian person information. This will enable the Rights Administrator to verify that they have chosen the intended machine account to assign access roles to for the selected *participant*. If it is not the correct machine account, the Rights Administrator can use the “Go back” button to enter and search for the right one to use.

## New Machine Account

When a Rights Administrator chooses the process to create a new machine account they will be navigated to the “Create Machine Account for Access Role Grant” page as shown by the example in Figure 8-39. The Rights Administrator must provide the IP Address assigned to the *participant* workstation or server where this machine account will be used so that the *IESO* can use it in defining firewall rules to permit communications between the selected *participant* workstation or server and *IESO* systems. The rationale is that machine account passwords assigned by the custodian after receiving an IESO Gateway activation email and creating the user account will typically be enduring and potentially more subject to a breach of security so firewall rules at the *IESO* will limit the use of the machine account to the registered *participant* system.

Once the Rights Administrator enters the *participant* IP address to be associated to the new machine account and clicks on the “Next” button, they will be navigated to the “Search for a Registered Person” page as shown in Figure 8-28 to start the process to choose a Custodian for the machine account. Through the person selection process the Rights Administrator can choose to either choose

to assign an existing person to the machine account as custodian or register a new person as custodian as shown in Figures 8-29 through 8-31.

The screenshot displays the 'Create Machine Account for Access Role Grant' page. At the top, there is a navigation bar with 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions' (highlighted). The user is identified as 'Richard RightsAdmin'. The IESO logo is on the left. The main content area is titled 'Create Machine Account for Access Role Grant' and includes the instruction: 'Please enter the enrollment information for this new machine account.'

**Request Details**

- Organization ID: 109120
- Organization Name: BJ ENERGY LLC
- System Access Request Type: Grant Access Role(s)
- Account Type: Machine

**New Machine Account Information**

Please provide the IP (Internet Protocol) address for the API to be associated with this new machine account.

IP Address:

Buttons: Go Back, Next, Cancel

\*Required

**Figure 8-39: Create Machine Account for Access Role Grant Page**

Once the Rights Administrator has either:

- Confirmed an existing machine account to be used or
- Chosen or entered the custodian person associated with the new machine account

he or she will be navigated to the 'Select Access Role(s) to be Granted' page for the machine account as shown by the example in Figure 8-40.

For revocation of access role requests for existing machine accounts the Rights Administrator will be navigated to a 'Select Access Role(s) to be Revoked' page similar to that shown by Figure 8-34 except that only machine account access role associated to the account will be available for selection.

**Select Access Role(s) to be Granted**

**Request Details**

Organization ID 999999  
 Organization ACME GENERATION  
 System Access Grant Access Role(s)  
 Request Type  
 Account Type Machine  
 Person F. Allen Wiley  
 (Custodian)  
 Person ID 507370  
 Machine Account APIIESO00014  
 Id

**Existing Access Role(s)**

Role Name	Description
No items available	

1-1 of 0

**Access Roles**

Select Access Role(s) to assign. The access role(s) listed correspond to the access role(s) that may be needed based on the organization's participation.

**Financial Market Operations/Settlements**

<input type="checkbox"/>	Role Name	Description
<input type="checkbox"/>	Financial Market Reports API	Retrieve financial market reports via the IESO Participant Reports site.

1-1 of 1

**Participation Settlements**

<input type="checkbox"/>	Role Name	Description
<input type="checkbox"/>	Settlements Reports API	Retrieve settlement reports via the IESO Participant Reports site.

1-1 of 1

**Next** **Cancel**

\* Required

**Figure 8-40: Select Access Role(s) to be Granted – Machine Account Page**

The information displayed for an existing machine account/custodian being processed for a new grant or revoke access role will show any existing access roles (that the machine account/custodian is associated with) for the *participant* organization.

The “Select Access Role(s) to be Granted” page(s) will only display machine account related access roles associated to the Market or Program participation that the organization has registered for. This is to prevent unintended ‘grant’ requests from being submitted to the *IESO* for the *participant* machine

account. If an access role is not shown that the Rights Administrator thinks should be there, he or she should contact *IESO* Customer Relations. It is possible that a technical problem could exist or it may be possible that the *participant* needs to register for additional Markets or Programs.

The Rights Administrator should in the case of granting access roles to the machine account, choose only the required access roles (i.e. those authorized for the machine account by the *participant*) by check marking them and clicking on the “Next” button. Multiple access roles available may be displayed by the first, next previous and last arrow buttons shown on the page.

Once the Rights Administrator has clicked on the “Next” button she or he will be navigated to a “Confirm Access Role(s) to be Granted” page as shown in Figure 8-41.

The screenshot shows the IESO system interface. At the top, there is a navigation bar with 'News', 'Tasks (4)', 'Records', 'Reports', and 'Actions'. The user is identified as 'Richard RightsAdmin'. The main heading is 'Confirm Access Role(s) to be Granted' with a sub-heading 'Please confirm the access that will be granted to this person or machine account with this request.'

**Request Details**

- Organization ID: 999999
- Organization Name: ACME GENERATION
- System Access Request Type: Grant Access Role(s)
- Account Type: Machine
- Person (Custodian): F. Allen Wiley
- Person ID: 507370
- Machine Account ID: APIIESO00014

**Access Role(s) to be Granted**

Access Roles to Confirm for Account

Role Name	Description
Financial Market Reports API	Retrieve financial market reports via the IESO Participant Reports site.
Settlements Reports API	Retrieve settlement reports via the IESO Participant Reports site.

Navigation: 1-2 of 2

Buttons: Go Back, Confirm, Cancel

**Figure 8-41 Confirm Access Role(s) to be Granted – Machine Account Page**

The page will show the access roles selected to be granted and the Rights Administrator can use either the “Go Back” button to correct the selected access roles or click on the “Confirm” button and continue the process. Once confirmed the system will associate the access roles to the machine account for the *participant* organization chosen and send an automated provisioning grant request to the IESO Gateway system to enroll the actual machine account in the access roles requested.

For revoke access role(s) requests for machine accounts upon selection by the Rights Administrator of the required access roles to be revoked and clicking on the “Next” button (or use of the “Revoke All” button) she or he will be navigated to a Confirm Access Role(s) to be Revoke page similar to that shown in Figure 8-35. The page will show the access roles selected for revocation and the Rights

Administrator can use either the “Go Back” button to correct the selected access roles or click on the “Confirm” button and continue the process. Once confirmed the system will process the access roles to be revoked for the machine account for the *participant* organization chosen and send an automated provisioning revoke request to the IESO Gateway system to remove the membership that the actual machine account has with the access roles requested.

### 8.1.4 Registration System Manage Contact Information

When a Rights administrator or any normal *participant* contact person chooses the “Manage My Information” task as shown in Figures 8-23 or 8-24 above they will be navigated to a “Choose an Action” page where they can select the “Update Person Information” selection in the dropdown selection list as shown in the example in Figure 8-42.



The screenshot shows a web interface for managing contact information. At the top, there is a navigation bar with tabs for 'News', 'Tasks', 'Records', 'Reports', and 'Actions'. The 'Actions' tab is selected. To the right of the navigation bar, the user's name 'Richard Rightsadmin' and the system name 'Appian' are displayed. Below the navigation bar, the main content area is titled 'Choose an Action For Richard Rightsadmin'. It contains a form with a dropdown menu labeled 'Action' and the selected option 'Update Person Information'. There are two buttons at the bottom right: 'Continue' (green) and 'Cancel' (grey). On the left side of the form area, there is a red asterisk and the word 'Required'.

**Figure 8-42 Choose an Action Page**

The user can then click on the “Continue” button to navigate to the “Update Person Information” page for their person record as shown in the example in Figure 8-43.

**Update Person Information For Richard Rightsadmin**  
Please make any updates to your person information below.

**Person Information**

Person ID	507437	* Main Email	test@test.ca
Position	<input type="text"/>	Alternate Email 1	<input type="text"/>
* First Name	Richard	Alternate Email 2	<input type="text"/>
* Last Name	Rightsadmin	* Address Line 1	1234 mystreet
Middle Name	<input type="text"/>	Address Line 2	<input type="text"/>
Preferred Name	<input type="text"/>	Address Line 3	<input type="text"/>
* Main Phone	123-123-5678	Address Line 4	<input type="text"/>
Alternate Phone 1	<input type="text"/>	* City	Toronto
Alternate Phone 2	<input type="text"/>	* Province/State	Ontario
Fax Number	<input type="text"/>	* Postal Code/Zip Code	M5V 3Y3
		* Country	Canada
		Contact Notes	<input type="text"/>

\* Required

**Figure 8-43 Update Person Information Page**

The Person information retrieved will be that currently active on the system. However, all changes are maintained in historical records within the system. All of the required mandatory fields will of course be populated and these can be edited with updated information but they cannot be made blank and then saved. It is up to each person to maintain their own person information so that it is current and accurate. Once a *participant* contact is satisfied with any updates they can click on the “Continue” button. This will navigate them to a “Confirm Person Information” page as shown by the example in Figure 8-44.

**Confirm Person Information For Richard Rightsadmin**  
Ensure your information has been entered correctly as it may be used to send confidential information.

**Person Information**

Person ID	507437	Main Email	test@test.ca
Position		Alternate Email 1	
Given Name	Richard	Alternate Email 2	
Family Name	Rightsadmin	Address Line 1	1234 mystreet
Middle Name		Address Line 2	
Preferred Name		Address Line 3	
Main Phone	123-123-5678	Address Line 4	
Alternate Phone 1		City	Toronto
Alternate Phone 2		Province/State	Ontario
Fax Number		Post Code/Zip Code	M5V 3Y3
		Country	Canada
		Contact Notes	

\* Required

**Figure 8-44 Confirm Person Information Page**

Where the information shown on the “Confirm Person Information” page is not correct or incomplete the *participant* contact can choose to use the “Back” button to go back and edit the data and then use the “Continue” button to go the confirm page.

If the *participant* contact is satisfied with the ‘person’ information as shown on the page, he or she can choose to click on the “Finish” button. This will commit the data to the Online IESO Registration system.

For name, main phone and main email attribute updates committed to the Registration system; the system will automatically and transparently generate a provisioning change request in the background to the IESO Gateway system to update to any associated user accounts linked to the person record with those attribute values. This will ensure that any user personal and machine account information is kept up to date immediately as well.

**– End of Section –**

## 9. Use of Account Provisioning Tools

### 9.1 Use of the Password Change & Reset Functions

Passwords used with User Accounts issued for use with the IESO Gateway, Online IESO system, Reports site, Energy Market Interface (EMI), Prudential system and CROW Outage Management system etc. can be changed or reset via 4 separate methods.

- Password setup on account initialization / first time login to the IESO Gateway Once the password has been setup on login to the Gateway, the account may be used with the Online IESO system, IESO Workspaces (replaces IESO Portal Collaboration and Watchdox), Transmission Rights Auction, Prudential Manager, IESO Reports site, Energy Market Interface, Dispatch Service or CROW Outage Management system etc., depending on the access permissions the user has been granted.
- Password Self Recovery during Gateway system login when a user as Forgotten their Password. The user must have already selected their multifactor authentication options and the security question and answer to do this self-recovery.
- Request to the IESO Customer Relations to have their password reset and a new temporary password issued to the user via email.
- Password normal manual change after login via the IESO Gateway 'Security Profile' password change capability located on the 'Security Profile' user dashboard page.

The IESO Gateway User Guide also provides details on all of the above.

**Note:** The IESO Gateway, Online IESO, IESO Reports Site, Energy Market Interface and CROW Outage Management System etc. all use common User Accounts. Change to the password for a User Account within the Gateway for example will automatically be applicable and usable for the Online IESO system, Transmission Rights Auction, Prudential Manager, IESO Reports site, Energy Market Interface, Dispatch Service and CROW Outage Management System etc.

The user will upon account initialization and logging in to the IESO Gateway for the first time, select the multifactor authentication options and a security question and answer to be used for password self-recovery and stronger authentication when login circumstances warrant (i.e. different workstation used than normal or account used at abnormal time of day etc.).

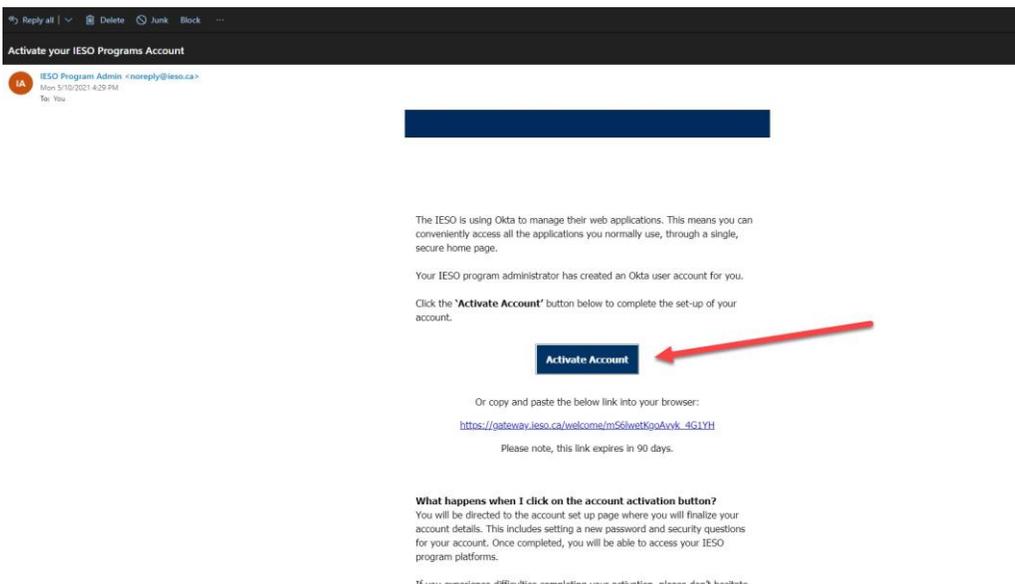
- Multifactor authentication may be presented to the user during each subsequent login to the Gateway depending on circumstances. The method used will be based on what the user selected during account initialization; i.e. Okta Verify, SMS Authentication, Email Verification, or Security Question.
- The security question can be selected from a randomly produced short list from a larger number of possible predefined choices. The choices shown available should meet all users' possible circumstances.
- Once the MFA options and security question have been selected and answer input, the MFA and question choices can be changed after Gateway logon at any time via the Security Profile page in the IESO Gateway.
- The answer to the security question is not 'case sensitive' and can use any ASCII characters. However, the user should select the security question that permits them to best

enter an answer that has personal meaning in order to be easily remembered but at the same time not easily guessed by someone else.

### 9.1.1 User Account Initialization

If the user needs to login for the first time to the IESO Gateway system (production or sandbox environment) for access to a secure IESO web server, they will have first received an activation email from the corresponding Gateway system with a link that can be used to initiate the process to activate the account. For IESO Workspaces (or FIT and MicroFIT) the account will be email address based while for all other market facing systems the account will be UserID based.

1. The end user should click on the “Activate Account” button in the body of the e-mail message as shown in Figure 9-1. This will navigate the end user to the referenced Gateway environment (Prod or Sandbox) web page to start the process for activating the account.



**Figure 9-1: Gateway Activation Email – Activate Account Link**

2. On the Gateway page navigated to, the end user should create a password for their user account that, at minimum, meets the requirements listed and then click on the “Create My Account” button at the bottom of the page to proceed as shown in Figure 9-2 and add the mobile phone number for use in resetting their password or unlocking their account via SMS where possible.

Enter new password

.....

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Your password cannot be any of your last 4 passwords

Repeat new password

.....

Add a phone number for resetting your password or unlocking your account using SMS (optional)

Okta can send you a text message with a recovery code. This feature is useful when you don't have access to your email.

+ Add Phone Number

Create My Account

**Figure 9-2: Gateway Activation Email – Activate Account Page**

3. The end user will then need to configure their MFA (multifactor authentication) Options, starting with SMS (Text Message), by clicking on the “Configure Factor” button as shown in Figure 9-3

ieso  
Connecting. Better. Powering. Enterprise.

Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Setup required

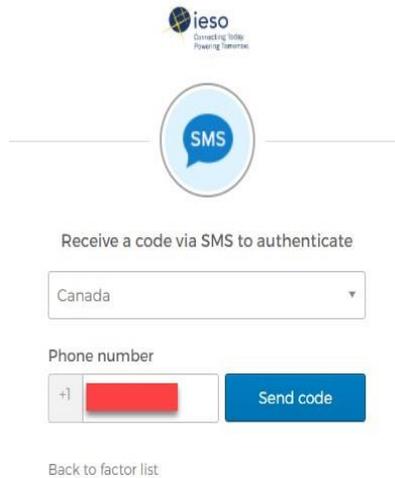
SMS Authentication   
Enter a single-use code sent to your mobile phone.

Security Question

Configure factor

**Figure 9-3: Gateway Multifactor Authentication Options Setup**

4. First choose a country and enter a valid phone number that can receive SMS (Text Message), then click on the “Send Code” button as shown in Figure 9-4. The mobile phone should receive an SMS message from the IESO Gateway system with a numeric code.



ieso  
Generating Value  
Powering Tomorrow

SMS

Receive a code via SMS to authenticate

Canada

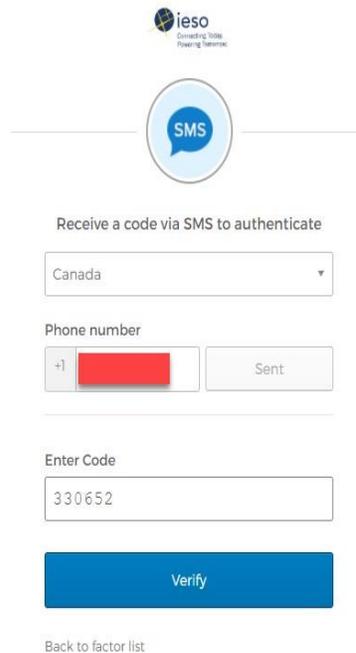
Phone number

+1 [Redacted] Send code

Back to factor list

**Figure 9-4: SMS Message Country and Phone Number Setup**

5. Enter the code received via SMS (Text Message) and click the “Verify” Button:



ieso  
Generating Value  
Powering Tomorrow

SMS

Receive a code via SMS to authenticate

Canada

Phone number

+1 [Redacted] Sent

Enter Code

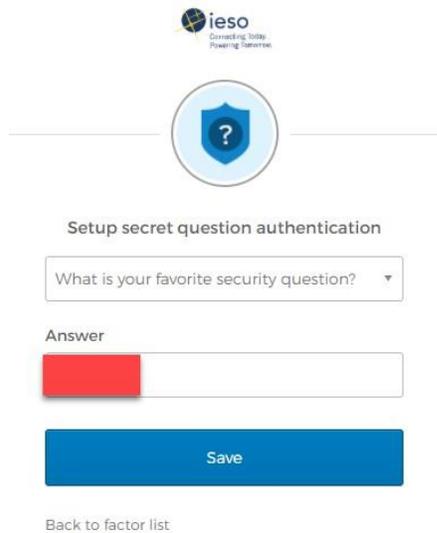
330652

Verify

Back to factor list

**Figure 9-5: SMS Code Receipt and Entry Verification**

- Next Configure the Security Question and Answer Multi Factor Authentication Prompt and click “Save”



The screenshot shows the IESO logo at the top, followed by a shield icon with a question mark. Below this is the heading "Setup secret question authentication". There is a dropdown menu with the text "What is your favorite security question?". Underneath is an "Answer" field with a red highlight on the left side. A blue "Save" button is positioned below the answer field. At the bottom, there is a link that says "Back to factor list".

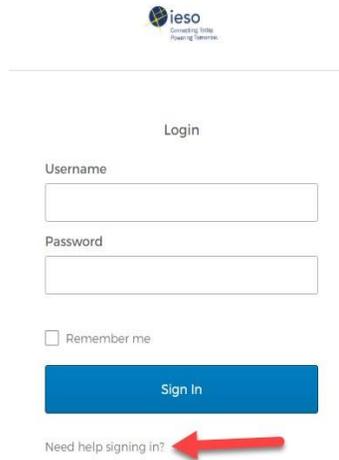
**Figure 9-6: Security Question and Answer Input**

- Once the Multi Factor Authentication Factors are configured, the end user should click on the “Finish” button presented in order to complete login and be navigated to the Gateway User Dashboard.

### 9.1.2 Self-Service Password Reset

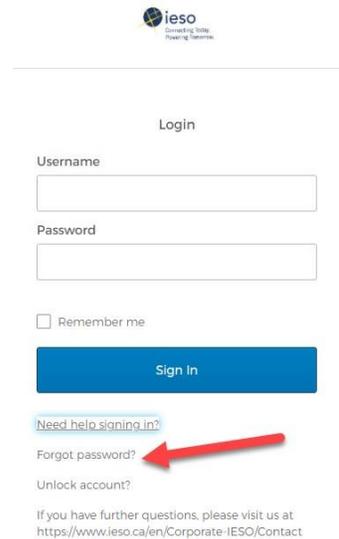
If an end user has forgotten their password, they can attempt a Self-Service password reset via the “Forgot Password?” Link on the login page. There are a number of options for resetting the password.

1. First the user should click the “Need help signing in?” text at the bottom of the login box as shown in Figure 9-7.



**Figure 9-7: Login Page – Need Help Signing in Link**

2. Next click on the “Forgot password?” link shown in Figure 9-8.



**Figure 9-8: Login Page – Forgot Password Link**

3. The end user should enter their e-mail or Username in the field specified. Email for email type account (used for IESO Workspaces) or Username for UserID type account (used for Market facing applications).
4. If the end user had previously added a mobile number for password reset purposes, the user can use the SMS (Text Message) option to reset their password by clicking the “Reset via SMS” button as shown in Figure 9-9. Then they can enter the code they receive via SMS text message, and click the “Verify” button.

The screenshot shows two stages of the IESO password reset process. The left stage, titled "Reset Password", features the IESO logo at the top. Below it is a text input field labeled "Email or Username" containing a redacted name. A note states: "SMS can only be used if a mobile phone number has been configured." There are two blue buttons: "Reset via SMS" (highlighted with a red arrow) and "Reset via Email". A "Back to Sign In" link is at the bottom. The right stage, titled "Enter verification code sent via SMS", also has the IESO logo. It shows an "Enter Code" input field next to a "Sent" button. Below is a large blue "Verify" button. A link "Didn't receive a code? Reset via email" and a "Back to Sign In" link are at the bottom.

**Figure 9-9: Reset Password – Reset Method Choice**

5. Alternatively, if the end user had NOT previously added a mobile phone number for password reset purposes they can use the “Reset via Email” button option to use e-mail in their profile to reset the password as shown in Figure 9-10. Then they can click on the “Reset Password” link in the e-mail received.

The screenshot shows the IESO logo at the top. Below it, the text "Email sent!" is displayed. A message states: "Email has been sent to [redacted] with instructions on resetting your password." Below the message is a large blue button labeled "Back to Sign In".

**Figure 9-10: Reset Password – Reset Via Email**

6. The end user can then enter a new password that meets the requirements, and click the “Reset Password” Button on the page that is displayed.
7. If completed successfully the user will be directed into the IESO Gateway User Dashboard. If not, they should contact IESO Customer Relations.

### 9.1.3 Temporary Password Change by IESO Customer Relations

There might be a situation where the end user cannot recover their own password and will need to have it reset by an IESO Customer Relations administrator.

**\*\*Please note: This option should only be considered after attempts to follow the Self Service Password Reset steps above have failed. Also refer to the Troubleshoot section at the end of this guide.**

In order to initiate the “Password Reset by Customer Relations” process, the end user must start by sending an e-mail requesting a password reset to [customer.relations@ieso.ca](mailto:customer.relations@ieso.ca). They should include as much details as possible in this e-mail such as full name, phone number, email address, organization where applicable, registration PersonID value, and account login value, but at minimum the request must include either:

The E-mail Address associated with the email based Okta / IESO Gateway Account

OR

The UserID value for the Username based Okta / IESO Gateway Account (if applicable)

This way the Customer Relations administrators will be able to assist the end user as quickly and as efficiently as possible.

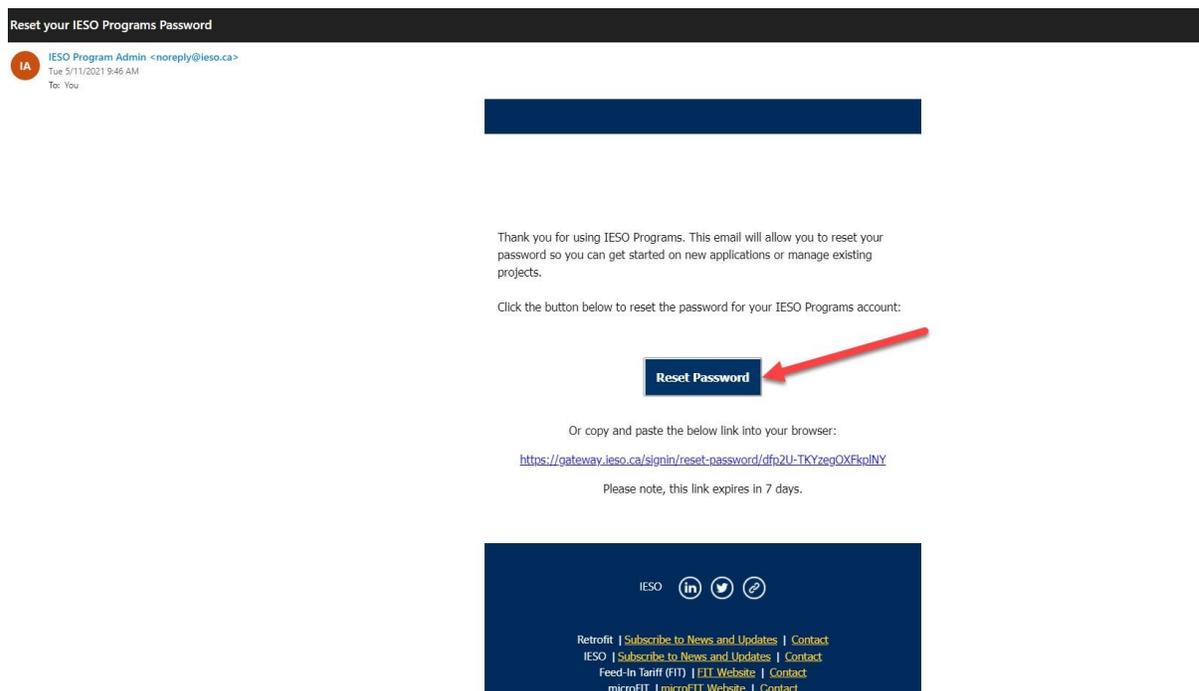
Once that is request has been submitted, there are 2 ways in which a Customer Relations administrator can assist the end user to recover / reset their account password. One of these ways is via the use of a Password reset e-mail to the end user. The other is by providing the end user with a temporary password directly via phone call.

## Customer Relations Reset Password Email

When the Customer Relations administrator resets the end user’s password, they should receive an e-mail with a “Reset Password” button.

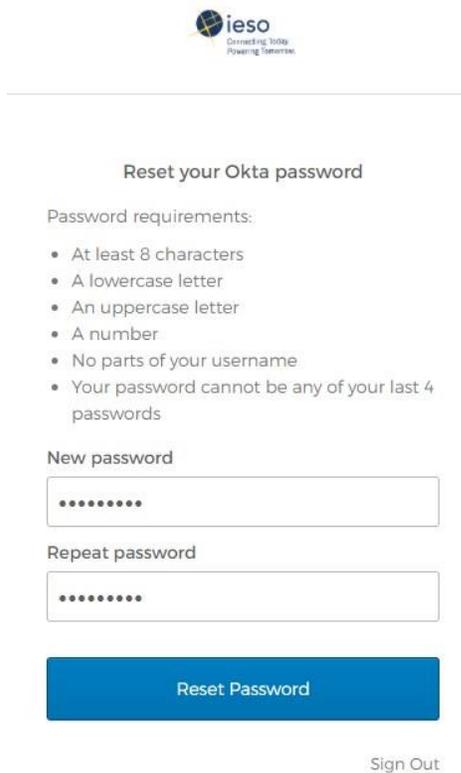
Upon receipt of this e-mail, the end user can perform the following steps in order to reset their password:

1. Click on the “Reset Password” button in the e-mail body as shown in the example in Figure 9-11. Note that the URL in the address provided in the email should start with “<https://gateway.ieso.ca>” for the production environment or “<https://gateway-sbx.ieso.ca>” for the sandbox environment. If it does not in the message or the actual page navigated to does not match, then the email should not be considered valid and Customer Relations should be contacted.



**Figure 9-11: Customer Relations Reset Password – Reset Via Email**

2. When navigated to the web page for the new password entry first validate the URL is valid then type in a new password that meets the rules / requirements listed and click the ‘Reset Password’ button as shown in the example in Figure 9-12.



**Reset your Okta password**

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Your password cannot be any of your last 4 passwords

New password

Repeat password

**Reset Password**

[Sign Out](#)

**Figure 9-12: Customer Relations Reset Password via Email – Password Reset Page**

3. Upon entry of the new password value and resetting, the end user’s new password will be set and they will be directed to the IESO Gateway User Dashboard.

### Customer Relations Reset Password – Temporary Password

Alternatively, if the end user’s password is reset by a Customer Relations administrator, they will be given a temporary password via phone call which the end user can use one time to set up a permanent password.

When the end user has typed in a temporary password, the system will continue to the “Reset Your Password” page. When creating a new password, the end user must choose one that meets the criteria provided on the page. It should be easy for to remember, but difficult for anyone else to guess. It is good practice to avoid dictionary words in any language and to use a combination of upper case and lower case letters, numbers and symbols. The longer it is the more secure it is.

In order to set a permanent password using the temporary password, the end user should follow these steps:

1. Open a web browser and navigate to <https://gateway.ieso.ca> if a production account is involved. Use <https://gateway-sbx.ieso.ca> if a Sandbox account is involved.

\*\*Ensure that an IESO supported browser is being used and operating system as listed on the Supported Client Platform page available on the IESO Corporate website at: <https://ieso.ca/en/Sector-Participants/Supported-Client-Platforms>.

2. The end user must ‘Sign In’ using the target subject account’s (email or UserID based) username involved and then the temporary password that was provided to them as shown in the example in Figure 9-13.

**Figure 9-13: Login Page Using Temporary Password**

3. On the subsequent resulting page presented the end user must ‘enter the temporary password again that was provided to them as shown in the example in Figure 9-14. The system knows that the password is a one-time temporary one and so will prompt the user to do so.

**Figure 9-14: Password Reset – Entering Old Temporary Password**

- The end user must then enter a new password meeting the rules twice and click on the ‘Change Password’ button as shown in Figure 9-15 to complete the set-up of the new password.

Your Okta password has expired

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Your password cannot be any of your last 4 passwords

Old password

New password

Repeat password

[Change Password](#)

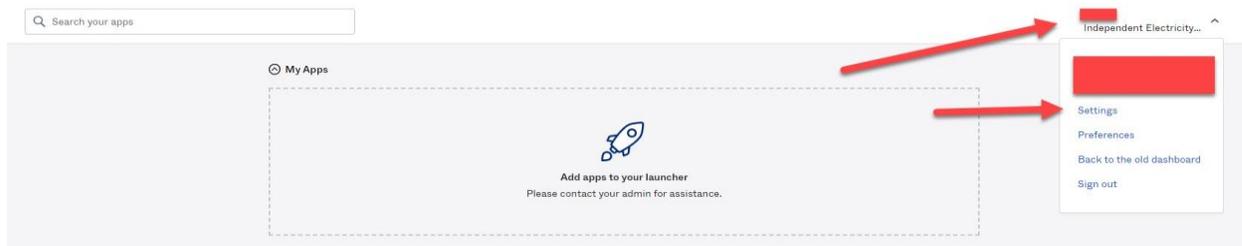
[Sign Out](#)

**Figure 9-15: Password Reset – Entering New Password**

### 9.1.4 User Security Profile Options

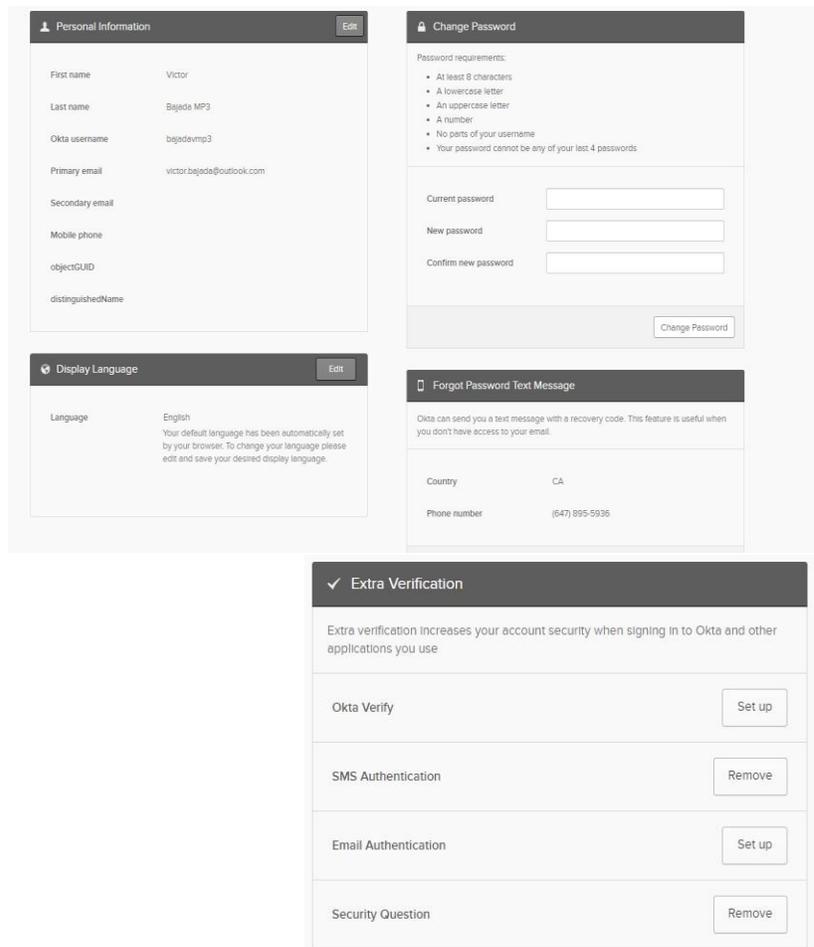
At any time during the lifecycle of the end user’s Identity Provider account, the end user can manage their user security profile options from the IESO Gateway User Dashboard.

- After logging in to the IESO Gateway (Prod or Sandbox) in order to access the profile, the end user can click on their name in the top right hand corner of the Dashboard and then click on the “Settings” button in the dropdown menu as shown in the example in Figure 9-16.



**Figure 9-16: IESO Gateway – User Dashboard Settings**

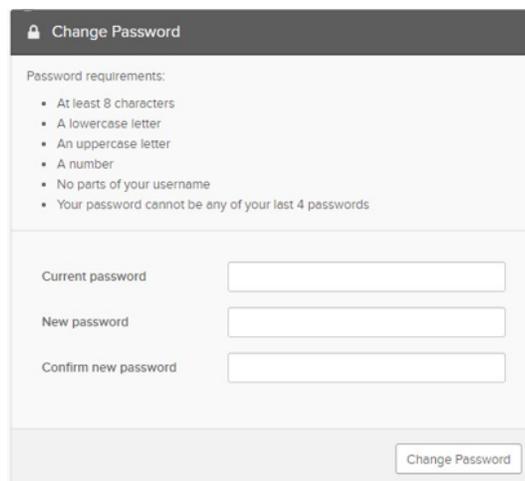
- Here the end user can manage settings such as, change password, some other aspects of their profile information, Display Language and MFA forgot password and other verification options as shown in the example in Figure 9-17.



**Figure 9-17: IESO Gateway – User Profile Settings Options**

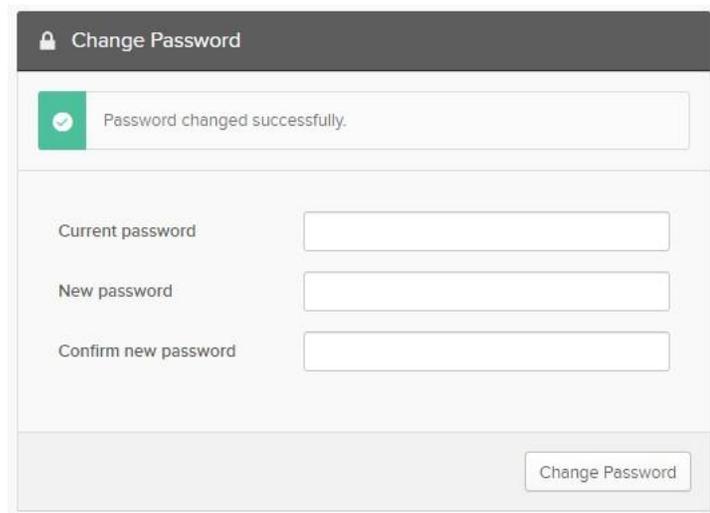
### **IESO Gateway – Security Profile Change Password**

1. To change their current password, the end user can enter the current password into the “current password” box as shown in Figure 9-18.

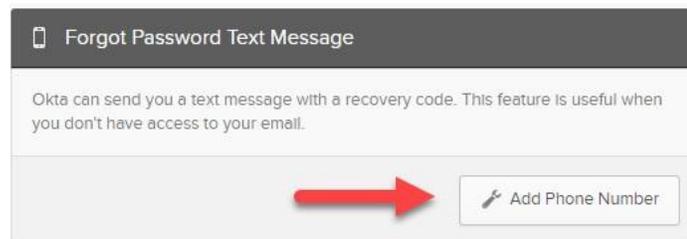


**Figure 9-18: Security Profile - Change Password**

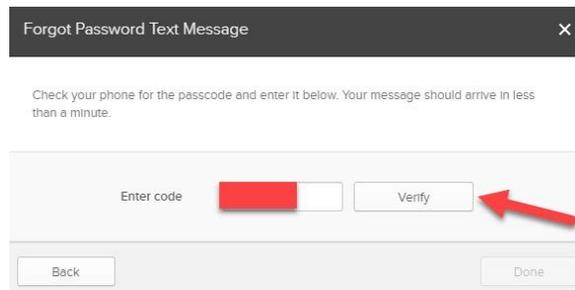
2. Then enter a new password and confirm by entering it again; so that it meets the requirements listed in the “Change Password” window. After clicking on the “Change Password” button, if done correctly the end user will receive a message saying “Password changed Successfully” as shown in Figure 9-19. If the password does not need the rules or is not entered the same twice and appropriate message will be displayed and the end user can try again.

The screenshot shows a web interface titled "Change Password". At the top, there is a green checkmark icon and the text "Password changed successfully." Below this, there are three input fields labeled "Current password", "New password", and "Confirm new password". At the bottom right, there is a button labeled "Change Password".**Figure 9-19: Security Profile - Change Password Result****IESO Gateway – Security Profile Forgot Password Text Message**

1. To set up a “Forgot Password Text Message”, the end user can click on the “Add Phone Number” button in the “Forgot Password Text Message” window if not already done so as shown in Figure 9-20.

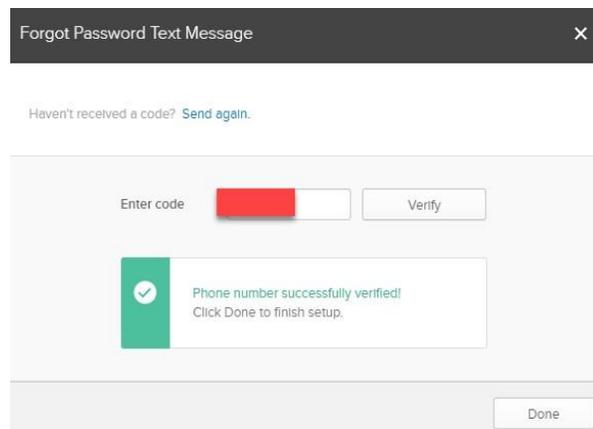
The screenshot shows a web interface titled "Forgot Password Text Message". It contains a paragraph of text: "Okta can send you a text message with a recovery code. This feature is useful when you don't have access to your email." Below the text, there is a button labeled "Add Phone Number" with a red arrow pointing to it.**Figure 9-20: Security Profile – Forgot Password Text Message - Add Phone Number**

2. In the resultant pop-up window, the end user should select a country and enter a valid phone number that can receive Text Messages such as their mobile phone number, then click on “Send Code”.
3. Upon receipt of the text message with the code, the end user must enter the code received and then click on the “Verify” button as shown in Figure 9-21.



**Figure 9-21: Security Profile – Forgot Password Text Message – Verification Code**

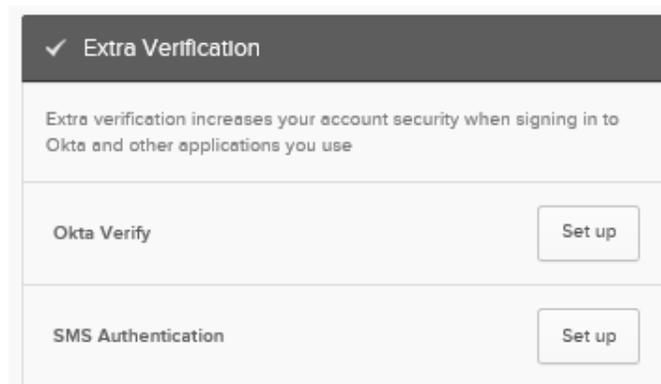
4. If completed successfully, the end user should receive a message saying “Phone number successfully verified as shown in Figure 9-22.



**Figure 9-22: Security Profile – Forgot Password Text Message – Phone Number Verified**

### IESO Gateway – Security Profile Additional MFA Options

1. To add additional MFA options, the end user can click on the “Set Up” button next to the Multifactor option they wish to configure as shown in Figure 9-23.



### Figure 9-23: Security Profile – Extra Verification Options

2. The end user will need to follow the instructions in the prompts for each of the MFA verification options.

\*\* Please note, if using Okta Verify, the end user will need to download the app from the respective App Store (i.e. Apple App Store, Google Play Store) before attempting to setup and use this option factor.

#### 9.1.5 Troubleshooting

If an end user has an IESO User account and they are having problems logging in, they should ensure the following are in place before contacting IESO Customer Relations:

- The end user should use the ‘Sign In’ links located here: <https://gateway.ieso.ca> (Production) or <https://gateway-sbx.ieso.ca> (Sandbox).
- The end user should ensure that they are using the IESO supported browser and operating system as listed on the Supported Client Platform page available on the IESO Corporate website at: <https://ieso.ca/en/Sector-Participants/Supported-Client-Platforms>
- The end user should ensure that they do not have Caps Lock or Unlock turned on with the keyboard.
- If the end user is unable to access an application once they are navigated to the IESO Gateway landing page / dashboard, they should check with their company’s registered Applicant Representative or Rights Administrator to ensure that they were registered in Online IESO Registration to access the application. Refer to [IESO Roles and Responsibilities](#) page on the IESO corporate website for more information.

If the end user is still experiencing issues, they should send any relevant screen shots of the error(s) encountered to [customer.relations@ieso.ca](mailto:customer.relations@ieso.ca) with an appropriate explanation of the problem.

For more information or assistance, please contact IESO Customer Relations:

Telephone: (905) 403-6900

Toll Free: 1-888-448-7777

E-mail:

[customer.relations@ieso.ca](mailto:customer.relations@ieso.ca)

**- End of Section -**

# 10. Browser Use

---

## 10.1 Browser Versions

Please refer to the supported client platform page on the IESO corporate website for browser makes and versions.

See supported client platforms on the corporate website at this [address](#)

– End of Section –

# 11. MIM Application Web Services

## 11.1 Introduction

The Market Information Management (MIM) system is one of the Web systems that allow the *participant* to interface with the *IESO*. Specifically, the MIM represents the secure internet-based client gateway to functionality provided by the *IESO* energy bidding system.

The *market participants* can interact with the MIM using the following two methods:

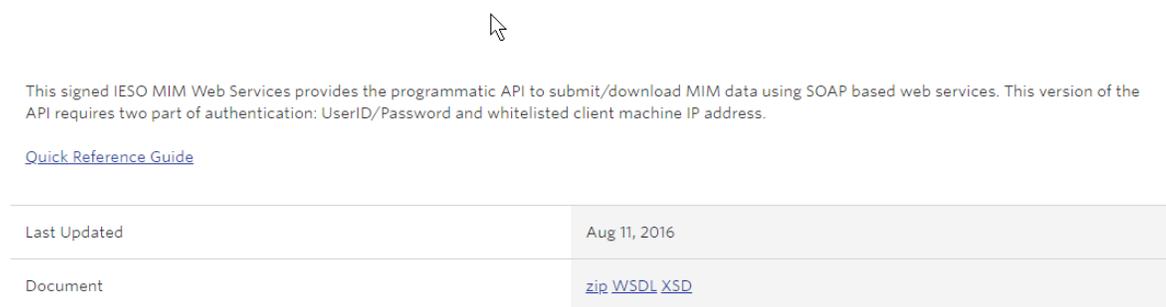
- Edge or Chrome browser to access the Energy Market Interface (EMI) web server via the new IESO Gateway. The browser is GUI based and interprets tag languages such as HTML. It allows client interaction through the keyboard/mouse; and
- The MIM Application Interface (Web Services) package. It allows Clients programmatic access to the MIM functionality via Web Services.

## 11.2 Downloading the MIM Web Services Files

Go to the Web site Technical Interface Page at this [address](#) using the Edge or Chrome Browser.

- 1) Choose and click on the “Market Participant Submissions (incl. MIM, EMI & API)” Link.
- 2) Scroll down to find the MIM Web Services listing as shown in Figure 11-1.

Market Information Management Application Interface (Web Services)



**Figure 11-1: Market Information Management Application Interface (Web Services)**

### Download

- 3) Click on the Web Services download link – ZIP as required.
- 4) Click on Save File when the prompt screen appears.
- 5) Using the save as option, choose a directory (ex: C:\Temp) to download the file (e.g.: MIM\_WebService\_Toolkit.zip) to.
- 6) Click on the Save button
- 7) Wait for the download to complete

Once downloaded, the zip file can be extracted to a directory of the developer’s choice. The Web Services Toolkit documentation is in the form of Word Document - MIM Web Service Toolkit (MWT) Guide.docx, which is located in the zip file.

**– End of Section –**

# Appendix A: Account Management Procedural Steps

This section contains detail on the tasks (steps) that comprise the Identity Management procedures. The steps in the following tables are illustrated in Section 4 above.

The table contains 3 columns, as follows:

**Ref.**

The numerical reference to the task.

**Task Name**

The task name as identified in Section 2 above.

**Task detail**

Detail about the task.

## A.1 Participant Account Application Scenario

A *participant* employee or contractor applies for a user account (personal or machine on Sandbox or Production) and system access roles / permissions via the *participant* Rights Administrator.

The steps in the following table are illustrated in the flow diagram entitled Participant User Account Application Scenario.

**Table A-1: Participant User Account Application Scenario Task Details**

Ref.	Task Name	Task Detail
A.01	Obtain Internal Approval and communicate contact role and Related system access requirement to Applicant Representative	A Credential Subscriber obtains internal <i>participant</i> approval as per the <i>participant's</i> processes and communicates as required to an Applicant Representative within the <i>participant</i> , the IESO system access requirements (Sandbox and/or Production environment). The Credential Subscriber should communicate to the Applicant Representative what access permissions they are internally approved for.
A.02	Submit request for User Account and Contact role(s) via Online IESO Registration System	The Applicant Representative logs in to the Sandbox and/or Production Online IESO Registration system(s) and performs the person and user account registration and the grant access / contact role(s) process as described in Section 8 of this document for the Credential Subscriber for a new registered person and the associated personal or machine account.
A.03	Receive and process Grant/Revoke access	The IESO Registration system receives the Grant/ Revoke access request from the Applicant Representative. It will validate the

Ref.	Task Name	Task Detail
	request and initiate automated account provisioning for creation of user account	request to ensure the account does not already exist (i.e. conflict with another person's personal or machine account). It will then initiate and automated provisioning request to the IESO Gateway system for a user account for the Credential Subscriber and enroll the account in the required role groups.  The Registration system will issue an email notification to the Credential Subscriber with the User Account Name used.
A.04	Receive automated account provisioning request for user account. Create account/enroll in role groups and issue activation email to Credential Subscriber	The IESO Gateway system will process the account creation and role group enrolment request and issue an activation email to the Credential Subscriber so they can initialize their account.
A.05	Receive notification email with User Account Name and Activation email with link to IESO Gateway. Continue on to account initialization to set password and configure MFA Options	The Credential Subscriber will receive a notification email from the registration system with their account UserID and an activation email from the IESO Gateway system. The Credential Subscriber can then proceed to the initialization process to setup their account password and multifactor authentication options as per section 9 of this document.

## A.2 Participant Account Change Scenario 1

Requesting a change to *participant* Individual Subscriber's or Application Subscriber's Information (Sandbox or Production) where:

- The requested change impacts system access roles for Individual or Application Subscriber's User Account (grant or revoke)

The steps in the following table are illustrated in the flow diagram entitled Participant User Account Change Scenario 1.

**Table A-2: Account Change Scenario 1 Task Details**

Ref.	Task Name	Task Detail
B.01	Obtain Internal Approval and communicate Contact roles requirement to Applicant Representative or system access requirement to Rights Administrator	A Credential Subscriber obtains internal <i>participant</i> approval as per the <i>participant's</i> processes and communicates as required to an Applicant Representative for contact role changes and./ or a Rights Administrator within the <i>participant</i> for IESO system access changes (Sandbox and/or Production environment). The Credential Subscriber should communicate to the Applicant Representative / Rights Administrator the existing user account information, Person ID and what contact roles / access permissions are internally approved for granting or revoking.
B.02	Submit request for a change to a Person's Contact roles permissions via Online IESO Registration System	The Applicant Representative submits a grant or revoke request for changes to a Person's Contact roles permissions via the IESO Online Registration System as per Section 8 of this document and informs the user of those changes. Participation contact role changes made should take effect immediately.
B.03	Submit request for a change to a user account's System access permissions via Online IESO Registration System	The Rights Administrator (or applicant representative) submits a grant or revoke request for changes to a user account's system access permissions (personal or machine account) via the IESO Online Registration System as per Section 8 of this document and informs the user of those changes.
B.04	Receive Grant/Revoke access request and update access/ contact roles registration and initiate automated account provisioning for changes in user account's role groups in authentication system.	The IESO Registration System upon receipt of the Grant/Revoke access request, updates the contact roles and system access registration information for the Credential Subscriber and where required initiates automated account provisioning with the IESO Gateway system for changes to the user account's role groups.
B.05	Receive confirmation of access / contact role changes and	The Credential Subscriber will receive confirmation of the access / contact role changes from the IESO Registration system where applicable and feasible.

<b>Ref.</b>	<b>Task Name</b>	<b>Task Detail</b>
B.06	provisioning results  Receive automated account provisioning request for user account. Make changes in role groups in Okta	The IESO Gateway system will receive the automated account provisioning request for the target user account. It will then make the required changes to the account's role group memberships in Okta

## A.3 Participant User Account Change Scenario 2

Requesting a change to *participant* Individual Subscriber's or Application Subscriber's Information (Sandbox or Production) where:

- The requested change is a Significant Change that impacts credential attributes for the person's User Account such as name, machine account custodian change, email address, phone number

The steps in the following table are illustrated in the flow diagram entitled Participant Account Change Scenario 2.

**Table A-3: Participant User Account Change Scenario 2 Task Details**

Ref.	Task Name	Task Detail
C.01	Update the person record in the IESO Online Registration System where applicable and confirm the changes in the system	An Individual or Application Subscriber ("machine account Custodian") updates their person record in the online Registration System where applicable and commits the changes to the IESO systems.
C.02	Receive Person change request task in Online IESO Registration. Validate and process person and user account change information. Submit changes to IESO Gateway system.	The IESO Registration System will receive the Person change request task. It will validate the request and process the person and user account changes and submit an automated provisioning request to the IESO Gateway system to update the Credential Subscriber's user account(s)  A notification email of the changes is sent to the Credential Subscriber
C.03	Receive automated account changes provisioning request for user account. Make changes to account for name, email address.	The IESO Gateway System receives the automated account changes provisioning request for the target account(s). It will make the required changes to the target account(s), (e.g. person name, email address, phone no.)  The IESO Gateway system sends an email notification to the end user of the implemented changes to the account.
C.04	Receive confirmation of account attribute changes provisioning results	The Credential Subscriber receives the person / account change information notifications from the IESO Registration System and IESO Gateway System.

## A.4 Participant User Account De-provisioning / Deactivation Scenario

A *participant* Rights Administrator requests a User Account de-provisioning / deactivation (Sandbox or Production) for a *participant* Individual or Application Subscriber where applicable.

The steps in the following table are illustrated in the flow diagram entitled Participant User Account De-provisioning / Deactivation Scenario.

**Table A-4: Participant User Account De-Provisioning / Deactivation Scenario Task Details**

Ref.	Task Name	Task Detail
D.01	Communicate removal of participant contact / access roles and system access permissions and desired account activation with Applicant Representative or Rights Administrator	A Credential Subscriber (or Primary Contact in cases where person has left <i>participant</i> ) communicates the need for removal of the selected person's contact roles and systems access permissions for the selected organization and where desired account deactivation with the Applicant Representative and / or Rights Administrator.
D.02	Remove selected person's participant contact roles for selected organization and where applicable request account deactivation via Online IESO Registration System	The Applicant Representative submits a revoke request of the person's contact role(s) for the chosen organization and where applicable request account deactivation via the IESO Online Registration System.  Participation contact role changes made, take effect immediately via the IESO Online Registration System.
D.03	Remove selected person's participant system access roles for selected organization via Online IESO Registration System	The Rights Administrator submits a revoke request of all access role(s) for all of the selected person's user account(s) for the chosen organization via the IESO Online Registration System.

Ref.	Task Name	Task Detail
D.04	Receive Grant/Revoke change request submitted by Rights Administrator. Validate and update registration records and submit de-provisioning changes to IESO Gateway system.	The IESO Registration System receives the Grant/ Revoke change request(s) from the Applicant Representative / Rights Administrator and validates and updates the registration records. It then submits automated deprovisioning changes to the IESO Gateway system and where applicable deactivation of the person's user account(s)
D.05	Receive automated account de-provisioning request for user account. Make changes to account and deactivate account(s) where no longer required.	<p>The IESO Gateway System will receive the automated account deprovisioning request arrange for disabling of the targeted person's User Account(s) systems access roles / privileges and deactivation of the User Account(s) where applicable.</p> <p><i>IESO ITOPS</i> Customer Support will notify the Rights Administrator of the disabling of the User Account(s) systems access roles / privileges for the <i>participant</i> and deactivation of user account where no longer required where applicable.</p>
D.06	Receive notification of removal of User Account's participant systems access and deactivation of account where no longer required	The Rights Administrator will receive notification of removal of User Account's <i>participant</i> systems access and deactivation of account where no longer required where feasible and applicable.

## A.5 Participant User Account Recovery Scenario 1

A *participant* Individual Subscriber or Application Subscriber performs an online recovery of their identity credential (Sandbox or Production) or requests the recovery of their identity credential via *IESO* Customer Relations.

The steps in the following table are illustrated in the flow diagram entitled Participant User Account Recovery Scenario 1.

**Table A-5: Participant User Account Recovery Scenario 1 Task Details**

Ref.	Task Name	Task Detail
E.01	Use Gateway online provisioning tools to recover credentials or replace forgotten identity credentials password using MFA SMS or email options. Else communicate need to recover account password to IESO Customer Relations	An Individual Subscriber or Application Subscriber initiates a self-recovery attempt for their User Account password with the IESO Gateway system's self-service password reset facility where possible.  If not possible the person can email or call <i>IESO</i> Customer Relations for support where self-recovery functionality is unsuccessful.
E.02	Receive account recovery request for user account. Validate request and issue recovery token via SMS or email.	The IESO Gateway system receives the account recovery request for the user account. It validates the request and issues a recovery token via SMS or email depending on the end user's chosen MFA options.
E.03	Arrange for recovery of User Account password so a temporary password or reset email is sent to the Credential Subscriber. Where applicable arrange for	<i>IESO</i> Customer Relations receives the email or phone call request from the Credential Subscriber, validates it is genuine and arranges for recovery of the User Account password so a temporary password or reset email can be sent to the Credential Subscriber.  They will arrange for unlocking of account where required.

Ref.	Task Name	Task Detail
	unlocking of account if required.	
E.04	Receive recovery email link / token for User Account password reset or temporary password from IESO Customer Relations. Reset password via IESO Gateway	<p>The Credential Subscriber will receive the recovery email link / token for a User Account password reset or the temporary password from IESO Customer Relations.</p> <p>The Credential Subscriber will then reset their password via the IESO Gateway.</p> <p>Where successful the process ends.</p>
E.05	Receive account recovery request for user account from Administrator. Validate request and permit temporary password setup	<p>The IESO Gateway system receives the account recovery request for user account from the IESO Customer Relations administrator. Its validates the request and permits a password reset for email activation or a temporary password setup.</p>
E.06	Validate reset of user account password based on SMS/email token or IESO issued temporary password	<p>The IESO Gateway system upon triggering by the email reset or temporary password from the Credential Subscriber validates the reset of user account password based on SMS/email token or IESO issued temporary password and completes the password reset.</p>

## A.6 Participant User Account Recovery Scenario 2

An existing Rights Administrator performs an online recovery of their identity credential (Sandbox or Production) or requests the recovery of their identity credential via *IESO* Customer Relations:

The steps in the following table are illustrated in the flow diagram entitled Participant User Account Recovery Scenario 2.

**Table A-6: Account Recovery Scenario 2 Task Details**

Ref.	Task Name	Task Detail
F.01	Use Gateway online provisioning tools to recover credentials or replace forgotten identity credentials password using MFA SMS or email options. Else communicate need to recover account password to IESO Customer Relations	A Rights Administrator will use the IESO Gateway online provisioning tools to recover credentials or replace a forgotten identity credentials password using their chosen MFA options. If this fails, the Rights Administrator can communicate the need to recover their account password with <i>IESO</i> Customer Relations via email or a phone call providing all necessary details that will let their request be validated.
F.02	Receive account recovery request for user account. Validate request and issue recovery token via SMS or email.	The IESO Gateway system will receive and validate the request to recover Rights Administrator account password and issue a recovery token via SMS or email depending on the end user's chosen MFA options.
F.03	Arrange for recovery of user Account password so a temporary password is sent to the Rights Administrator. Where applicable arrange for unlocking of account if required.	<i>IESO</i> Customer Relations receives the email or phone call request from the Rights Administrator, validates it is genuine and arranges for recovery of the User Account password so a temporary password or reset email can be sent to the Rights Administrator's and/or arrange for unlocking of the account where required.
F.04	Receive recovery email link / token for User Account password reset or temporary password from IESO	The Rights Administrator will receive the recovery email link / token for a User Account password reset or the temporary password from IESO Customer Relations.  The Rights Administrator will then reset their password via the IESO Gateway.

Ref.	Task Name	Task Detail
F.05	Reset password via IESO Gateway  Receive account recovery request for user account from Rights Administrator. Validate request and permit temporary password setup	Where successful the process ends.  The IESO Gateway system receives the account recovery request for user account from the IESO Customer Relations administrator. Its validates the request and permits a password reset for email activation or a temporary password setup.
F.06	Validate reset of user account password based on SMS/email token or IESO issued temporary password	The IESO Gateway system upon triggering by the email reset or temporary password from the Rights Administrator validates the reset of user account password based on SMS/email token or IESO issued temporary password and completes the password reset.

## A.7 Participant Rights Administrator Enrolment Scenario

A *participant* Primary Contact is requesting enrolment of a Rights Administrator in either Sandbox and/or Production environments.

The steps in the following table are illustrated in the flow diagram entitled Participant Rights Administrator Enrolment Scenario.

**Table A-7: Rights Administrator Enrolment Scenario Task Details**

Ref.	Task Name	Task Detail
G.01	Complete selected person's Rights Administrator role assignment for selected organization and create user account request via Online IESO Registration System where applicable.	<p>The Primary Contact at a <i>participant</i> completes the selected person's Rights Administrator role assignment for the selected organization in Sandbox and/or Production and in the process creates a user account request via the Online IESO Registration System (Sandbox and/or Production) where applicable. If the person already has an <i>IESO</i> user account (Sandbox and/or Production) the process is complete.</p> <p>If the person enrolled in the Rights Administrator for the <i>participant</i> does not have an <i>IESO</i> User Account the Registration System will generate an automated provisioning request to the IESO Gateway system to create the account.</p>
G.02	Receive Grant/Revoke access request from Primary Contact. Validate grant/revoke information. Update organization /contact roles registration and initiate automated account provisioning where applicable for user account creation and/or role groups in authentication system.	<p><i>The IESO</i> Registration System will receive a Grant/ Revoke access request from the Primary Contact. It will validate the grant/revoke information, then update the organization /contact roles registration information and initiate automated account provisioning where applicable for user account creation and/or membership in role groups in the IESO Gateway authentication system.</p> <p>If an account exists, the Participant Rights Administrator enrolment is complete.</p> <p>A registration notification email is sent to the Rights Administrator.</p>

<b>Ref.</b>	<b>Task Name</b>	<b>Task Detail</b>
G.03	Receive account provisioning request for user account. Create account and provision access roles and Issue activation email.	The IESO Gateway System receives an account provisioning request for a user account. It create the account and provisions access roles and then issues an activation email to the end user.
G.04	Receive activation email with User Account Name and link to IESO Gateway. Continue on to account initialization to set password and configure MFA Options	The Rights Administrator receives the registration email plus the activation email from the Registration system /IESO Gateway system with the User Account Name and the link to IESO Gateway system. He or she will continue on to account initialization to set up the account password and configure their MFA Options (Sandbox and/or Production Gateway system as applicable).

## A.8 Participant Rights Administrator User Account Change Scenario 1

An existing Rights Administrator is requesting a change to their information where:

- The requested change is a Significant Change that impacts credential attributes for the person's account such as name, machine account custodian change, email address, phone number

The steps in the following table are illustrated in the flow diagram entitled Participant Rights Administrator Account Change Scenario 1.

**Table A-8: Rights Administrator Change Scenario 1 Task Details**

Ref.	Task Name	Task Detail
H.01	Updates their person record in the Online IESO Registration system where applicable and in the process initiates a provisioning request to update their user account information.	The Rights Administrator Updates their person record in the Online IESO Registration system (Sandbox and Production) where applicable and in the process the Online IESO Registration System initiates a provisioning request to update their user account information.
H.02	Receive Person change request task in Online IESO Registration. Validate and process person and user account change information. Submit changes to IESO Gateway system.	The IESO Registration system receives the Person change request task. It validates and processes the person and user account change information. It then submits changes to IESO Gateway system to update the user account attributes where required and sends a notification email to the end user.
H.03	Receive automated account changes provisioning request for user account. Make changes to	The IESO Gateway system receives the automated account changes provisioning request for the user account. It then make changes to account for name, email address, phone no. as required and sends a notification email to the end user of the changes.

Ref.	Task Name	Task Detail
	account for name, email address, phone no.	
H.04	Receive confirmation of account attribute changes provisioning results	The <i>participant</i> Rights Administrator will receive the confirmation change notification email of his or her credential updates from the <i>IESO</i> Gateway system where possible.

## A.9 Participant Rights Administrator User Account Change Scenario 2

An existing Rights Administrator is requesting a change to system access permission changes (Sandbox and/or Production) for themselves or another Rights Administrator.

The steps in the following table are illustrated in the flow diagram entitled Participant Rights Administrator Account Change Scenario 2.

**Table A-9: Participant Rights Administrator Account Change Scenario 2 Task Details**

Ref.	Task Name	Task Detail
I.01	Obtain internal Participant approval for contact role /system access permission changes	The Rights Administrator obtains internal <i>participant</i> approval for contact role / system access permission change (Sandbox and/or Production). For contact roles the Rights Administrator has the Applicant Representative make the changes. In many Participants this may be the same person.
I.02	Submit request for a change to a Rights Administrator's Contact role permissions via Online IESO Registration System	An Applicant Representative a request for change to a Rights Administrator's (for same Participant) user account's access roles / Contact roles via the Online IESO Registration System (Sandbox and/or Production).  Participation contact role changes made, take effect immediately via the IESO Online Registration System. Some changes may require the Registration system to update the IESO Gateway system.
I.03	Submit request for a change to a Rights Administrator's system access permissions via Online IESO Registration System	A Rights Administrator submits a request for change their own or another Rights Administrator's (for same Participant) user account's access roles / system access permissions via the Online IESO Registration System (Sandbox and/or Production).  This will require the Registration system to update the IESO Gateway system.
I.04	Receive Grant/Revoke access request and update access/ contact roles registration and initiate automated account provisioning for	The IESO Registration system receives the Grant/Revoke access request and updates access/ contact roles registration records for the Rights Administrator and initiates any automated account provisioning for changes for the user account's role groups in the IESO Gateway authentication system. This should happen immediately.  An email is sent to the Rights Administrator regarding the changes.

Ref.	Task Name	Task Detail
	changes in user account's role groups in authentication system.	
I.05	Receive confirmation of system access / contact role changes and provisioning results	The <i>participant</i> Rights Administrator will receive confirmation of the changes (Sandbox or Production) to the access roles / system access permissions for the Rights Administrator user account.
I.06	Receive automated account provisioning request for user account. Make changes in role groups in Okta	The IESO Gateway system receives the automated account provisioning request for the Rights Administrator's user account and makes the required changes in memberships for the role groups in Okta.

## A.10 Participant Rights Administrator Role Termination Scenario

A Primary Contact is requesting the termination of a *Participant* Rights Administrator role for a person and potentially removal of access roles and User Account deactivation (Sandbox and/or Production).

The steps in the following table are illustrated in the flow diagram entitled Participant Rights Administrator Role Termination Scenario.

**Table A-10: Participant Rights Administrator Role Termination Scenario Task Details**

Ref.	Task Name	Task Detail
J.01	Request removal of selected person’s Rights Administrator role assignment and participant contact roles for the selected organization and where applicable request account deactivation via Online IESO Registration System	A Primary Contact requests removal of the selected person’s Rights Administrator organization role assignment for selected organization in the Registration System (Sandbox and/or Production) and where applicable requests removal of the person’s user account/ access role assignments and potentially account deactivation via the Online IESO Registration System where applicable.
J.02	Remove selected person’s Rights Administrator role and any requested participant contact roles for the selected organization. Send de-provisioning request for associated role groups and/or deactivation of user account	<p>IESO Registration system will receive a Grant/ Revoke change request from the Primary Contact (Sandbox or Production). It will then validate the Grant/Revoke information for the organization, contact and access roles to be revoked.</p> <p>If the person still need an IESO user account, the process is complete. If an account is no longer needed the Primary Contact can request end dating of the of the user account. Then the Registration System (Sandbox and/or Production) will automatically send an automated provisioning request to the IESO Gateway system to deactivate the user account.</p>

Ref.	Task Name	Task Detail
	where applicable	
J.03	De-provision requested access roles for target user account.  Deactivate user account where applicable.	<i>IESO</i> ITOPS Customer Support will arrange for removal of the person's User Account's Registration System access and other access privileges (Sandbox or Production) and deactivation of the account where applicable. They will then notify the Primary Contact of deactivation of user account and removal of system access privileges where possible
J.04	Receive notification of access role and account de-provisioning results.	Receive notification of access role and account de-provisioning results.

## A.11 Credential Subscriber User Account Initialization / Password Reset

Initialization of any Credential Subscriber's User Account or reset of the password for that account

Once the *participant* person is registered for a User Account through the Online IESO Registration System, he/she will receive a User Account activation email for their IESO Gateway account.

The User Account once activated, by the Credential Subscriber can be used immediately. If required, the Credential Subscriber can request a password reset online or via IESO Customer Relations.

For more information on system functionality relating to the tasks described below, refer to section 9 of this guide.

**Table A-11: Credential Subscriber, Account Initialization Task Details**

Ref.	Task Name	Task Detail
K.01	Access the web based identity management tool at <a href="https://gateway.ieso.ca">https://gateway.ieso.ca</a> as indicated in the activation / reset password email for initializing or resetting a User Account	<p>If not already done; upon receipt of User Account activation email for initial issuance or password reset email from IESO Customer Relations for account recovery:</p> <p>For a User Account / Password identity credential used with the IESO Gateway (Sandbox or Production where applicable); the <i>participant</i> person shall access the provided <i>IESO</i> Gateway URL (Sandbox or Production) for initializing/using a User Account. The person where required, use the IESO Gateway to perform password self-reset using the IESO Gateway or for resetting a temporary password provided by IESO Customer Relations with one of their own choosing.</p>
K.02	Use the Gateway web interface to either <ol style="list-style-type: none"> <li>1. activate the user account and set up MFA parameters or</li> <li>2. reset the password for an existing account</li> </ol>	<p>Use the IESO Gateway system (Sandbox or Production) to:</p> <ol style="list-style-type: none"> <li>1. activate the user account and set up MFA parameters via the supplied activation email or</li> <li>2. reset the password for an existing account using the IESO Gateway themselves or reset the password via an IESO Customer Relations supplied email or a temporary password provided orally</li> </ol>
K.03	Validate User Account activation information and permit user to setup password, multifactor authentication	The IESO Gateway will validate the User Account activation information and permit the end user to setup an enduring password, plus their multifactor authentication SMS/security question parameters.

Ref.	Task Name	Task Detail
	SMS/security question parameters	
K.04	Validate user account self-reset SMS code / email or IESO Customer Relations reset email parameters	<p>The IESO Gateway system will validate the user account self-reset SMS code / email or IESO Customer Relations reset email parameters and let the end reset their password.</p> <p><b>Note:</b> In the case where a user's account is locked it will be unlocked by IESO Customer Relations.</p>
K.05	Login to IESO Gateway to confirm account. Read Legal disclaimer and login. Complete MFA prompt.	<p>The User Account's successful password change / reset is confirmed within the Gateway login web pages to the end user. The user may have to answer an MFA prompt. The IESO legal disclaimer is available on the Gateway landing page for reference.</p> <p>When complete the person will be able to use the User Account to login to the IESO Gateway and access the applications the end user is authorized for.</p>

## A.12 Periodic Update of Subscriber User Account Password (where required) Scenario

Table A-12: Update of Account Passwords

Ref.	Task Name	Task Detail
L.01	Login to the IESO Gateway at <a href="https://gateway.ieso.ca">https://gateway.ieso.ca</a> with a User Account.  Sandbox URL is <a href="https://gateway-sbx.ieso.ca">https://gateway-sbx.ieso.ca</a>	For the IESO Gateway a User Account and password (Sandbox or Production) are used to login as normal. (Production URL - <a href="https://gateway.ieso.ca">https://gateway.ieso.ca</a> , Sandbox URL - <a href="https://gateway-sbx.ieso.ca">https://gateway-sbx.ieso.ca</a> ) may prompt t
L.02	Check for password renewal and initiate password update process if required.	Periodically if so configured the IESO Gateway may check for password renewal and initiate the process to do so to the end user
L.03	No notification of update needed at Gateway login. Use Gateway credentials as required for normal business operations.	If no notification of update is needed at Gateway login the end user can use Gateway credentials as required for normal business operations and the process ends.
L.04	Gateway identity management system sends User Account password change prompt to end user	Where a password update is needed the IESO Gateway sends the end user a prompt in the GUI login screens to change their password.
L.05	Change password in Gateway login screen using old password and or MFA options to enable change	The user shall follow the instructions on the IESO Gateway web pages to change their password to a new one that meets the password rules.
L.06	Validate user account password change with old password / MFA options	The IESO Gateway will validate the end user's responses using the chosen MFA options and old password to facilitate the password update.

---

<b>Ref.</b>	<b>Task Name</b>	<b>Task Detail</b>
		Upon successful password update the process ends or in case of failure the end user can contact IESO Customer Relations.

## A.13 Description of Changes

### A.13.1 Credential Subscriber Information

#### Types of Changes

Changes to Credential Subscriber information are differentiated on the basis of their impact on identity credential (User Account / Password).

**Contact or Access Role(s) change** – The requested change requires changes to a user’s system access permissions (grant or revoke) for any *IESO* contact or access role that the *participant* is valid for through their registered market and program participations. Some contact roles have no assigned system access permissions associated with them.

**Person and account information change** – The requested change requires a change to the identity credential issued to the requestor including first name, middle name, last name, phone number and email address.

Changes to the User Account password are handled under the password recovery / reset processes.

**Note:** A Significant Change due to actual name change may require re-proofing of the identity of the Credential Subscriber via the *participant* internal processes but this is not mandated by the *IESO*.

#### When to Submit a Change Request

All Credential Subscriber information retained by the *participant* person and Rights Administrator and/or Primary Contact contained within or represented by a User Account should always remain accurate. If a *participant* person and Rights Administrator and/or Applicant Representative or Primary Contact are aware of inaccuracies, a Registration system request should be submitted by the Applicant Representative / Rights Administrator.

## A.13.2 Rights Administrator Information

### Types of Changes

Changes to a Rights Administrator person's information are differentiated on the basis of their impact to the Rights Administrator role itself and on identity credential (User Account / Password).

#### Contact / Access Role(s) change

Changes to a person's Rights Administrator role (adding or removing the role to the person) will impact the person's Registration System access permissions.

Any other requested change requires changes to a user's system access permissions (grant or revoke) for any IESO access role that the *participant* is valid for through their registered market and program participations.

#### Person and account information change

The requested change requires a change to the identity credential issued to the requestor including first name, middle name, last name, phone number and email address.

Changes to the User Account password are handled under the password recovery / reset processes.

### When to Submit a Change Request

All Rights Administrator information retained by the *participant* Rights Administrator and/or Primary Contact contained within or represented by a User Account should always remain accurate. If a Rights Administrator, Applicant Representative or Primary Contact is aware of inaccuracies, a Registration system request should be submitted by the Applicant Representative / Rights Administrator.

– End of Section –

## Appendix B: Glossary of Terms

---

The following definitions and acronyms used within this guide are specific to *IESO* Identity Management.

**18 Month and Long-Term Assessments Contact** - Person responsible for data submissions for the 18-Month Outlooks and longer-term reliability assessments for their organization.

**Access Role Change** – is a change that does not impact credentials but impacts system access for a User Account.

**Application Subscriber** - is the term used for *participant* application/server system entity that will be using a User Account identity credential in combination with an API or system for access to an *IESO* Web site. An Application Subscriber is any application/server system that is associated with a service level User Account identity credential. Associated with the Application Subscriber is a Custodian.

**Bids and Offers Contact** - Section to be contacted regarding the bids or offers for your organization (24/7 - Operations Desk, Energy Trading Floor, Control Centre).

**Capacity Auction Contact** - Person responsible for all tasks related to capacity auctions.

**Communications and Customer Service Contact** - Person or Section responsible for receiving *IESO* information on communications and media issues and/or delivering customer service, for their organization.

**Compliance and Market Surveillance Contact** - Person responsible for discussing *participant* conduct and activities within the *IESO-administered markets* for their organization.

**Contributor Information Contact** - Person responsible for all tasks related to contributor information.

**Control Room Section** - Control room section for the participant organization.

**Credential Subscriber** - General term for Individual Subscriber or Application Subscriber.

**Custodian** - is normally the individual that owns and has rightful possession of the information. If the ownership has been delegated, the delegate has the rightful possession of the information and therefore is the custodian.

**Day-Ahead-Bids and Offers Contact** - Person or Section responsible for submitting and/or changing day-ahead bids or offers for their organization.

**Demand Response Auction Contact** - Person responsible for all tasks related to Demand Response Auction.

**Dispatch Data Submitter** - Person or Section responsible for submitting and/or changing the bids or offers for their organization.

**Dispatch Data Viewer** - Person or Section responsible for viewing and/or changing real-time bids or offers for their organization.

**Domain** - is the community consisting of the Subscribers.

**Emergency Preparedness Plan Contact**- Person responsible for submitting and updating the Emergency Preparedness Plan for their organization.

**Energy Limited Resource Forecast Contact** - Person responsible for submission of the energy limited resource forecast for their organization.

**Equipment Outage Submitter** - Person responsible for submitting, updating and canceling outage request on equipment owned or operated by their organization.

**Equipment Outage Viewer** - Person who can view outage information on equipment owned or operated by their organization, and equipment permitted for viewing by other organizations.

**Equipment Registration Specialist** - Person responsible to submit attributes to their equipment, facility and resources for your organization.

**E-Tag Curtailment Contact** - Person or Section responsible for receiving notifications regarding the limiting of energy flow on an arranged and/or confirmed interchange transaction for their organization.

**IESO Gateway System** – Okta based User Account and Access Management and authentication system is responsible for receiving user Account and system access role /permission requests and for performing account creation and issuance, name changes, access role changes and user Account deactivation and for authentication of all user account logins. Receipts of requests may be from the IESO Registration System via automated provisioning workflows or manually from IESO Access Management or IESO Customer Relations.

**Individual Subscriber** - is the general term used for *IESO* Identity Management individual end entities who apply for a User Account. An Individual Subscriber is any entity whose name appears as the subject in a User Account.

**Information Technology Contact** - Person or Section responsible for communicating with the IESO about information technology services, projects and changes for their organization.

**Invoicing and Banking Contact** - Person responsible for submitting and maintaining, or approving banking information for their organization.

**Market Participant Compliance Contact** - Person responsible for reliability compliance under the Ontario Reliability Compliance Program for their organization. This includes preparing and submitting Reliability Compliance Self-Certifications, periodic data submittals and data requests. In case of potential non-compliance, submitting Reliability Compliance Self-Reports and providing associated mitigation plans.

**Market Participant Escalation Contact** - Person responsible for reporting reliability compliance on escalated matters (due dates are missed) under the Ontario Reliability Compliance Program for their organization. This person is preferably of higher authority than the person designated as the Market Participant Compliance Contact.

**Meter Trouble Report Contact** - Person or Section responsible for monitoring metering data and the response of the Meter Service Provider, and responding to the late notification of Meter Trouble Reports for their organization.

**MMP Meter Trouble Report Contact** - Person responsible for monitoring Meter Trouble Reports, adding comments, and receiving Meter Trouble Reports status notifications.

**MSP Meter Trouble Report Contact** - Person responsible for responding to and initiating Meter Trouble Reports on meter issues and outages.

**MSP Revenue Metering Contact** - Person responsible for submitting meter registration requests, monitoring in-flight requests and data and viewing the master data for registered *meter installations*.

**Notice of Disagreement Contact** - Person responsible for submitting *Notices of Disagreement* for settlement statements for their organization.

**Message** - is a digital representation of a unit of information with a human readable equivalent. For example, a message may be a *participant's bid* or *offer* for an electrical market, pricing data, e-mail message or a file.

**Participant Primary Contact** – is an officer of a *participant* organization who is authorized by the Participant Authorized Representative to register Participant Rights Administrators on behalf of the *participant* organization. The Participant Primary Contact designates and delegates the role of the Participant Rights Administrator.

**Participant Rights Administrator** - means an employee of a *participant* Organization that is appointed by a Participant Primary Contact and is authorized to register for User Accounts and system access role/permissions for *participant* Individual Subscribers or Participant Application Subscribers requesting market systems access and an *IESO* identity credential.

**Participant Authorized Representative** - a senior officer at a *participant* organization who can authorize an officer (i.e., a high-level employee) of the *participant* organization to perform the responsibilities of a Participant Primary Contact.

**Password Recovery** – For a User Account identity credential this is handled by issuance of a new temporary password to the Credential Subscriber or for account used with the MIM Web Services, issuance of a new enduring password to the Credential Subscriber.

**Prudential Requirements Contact** - Person responsible for submitting prudential information and is the point of contact for any issues regarding Prudential information (margin calls, warnings and defaults) for their organization.

**Revenue Metering Contact** - Person responsible for viewing the master data for registered meter installations and in-flight data submitted during a meter registration request. The Revenue Metering Contact for a *transmitter* is also responsible for approving Site Registration.

**Revenue Metering Data Contact** - Person responsible for managing meter data report profiles, as well as requesting and retrieving revenue meter data reports for their organization.

**Settlements Contact** - Person responsible for issues/questions relating to *settlement statements* for their organization.

**Significant Change** - is a change in a user's credentials including change of first or last name, change of e-mail address, phone number or User Account value is no longer accurate.

– End of Section –

## Appendix C: List of Participations

---

The following participations currently exist within the Online IESO Registration system applicable to the Ontario wholesale electricity market. One or more participation contact roles that a person may be enrolled in; existing within Online IESO for each participation.

**Capacity Auction Participant** - The organization is eligible to participate in a capacity auction.

**Capacity Market Participant-MMP** - The organization is responsible for the financial settlements with respect to a resource with a *capacity obligation*.

**Capacity Market Participant-Operator** - The organization operates a resource with a *capacity obligation*.

**Capacity Market Participant-Owner** - The organization has a *capacity obligation*.

**Capacity Market Participant-RMP** – The organization submits dispatch data with respect to a resource with a *capacity obligation*.

**Central Service Provider** - No definition provided

**Centralized Forecasting Provider** - The organization provides a centralized forecasting service relating to variable generation.

**Centralized Forecasting-Variable Generator** - The organization participates in the Centralized Forecasting program to provide operational and meteorological data.

**Demand Response Auction** - The organization is eligible to participate in a Demand Response Auction.

**Demand Response Market Participant-MMP** - The organization is responsible for the financial settlements with respect to a Demand Response resource.

**Demand Response Market Participant-Operator** - The organization operates a Demand Response resource.

**Demand Response Market Participant-Owner** - The organization has a Demand Response Capacity Obligation.

**Demand Response Market Participant-RMP** – The organization submits dispatch data with respect to a Demand Response resource.

**Distributor-Metered Market Participant** - The organization is responsible for the financial settlement of metering data associated with a registered load facility.

**Distributor-Metered Market Participant Transmission Tariff** - The organization pays for one or more transmission services to a transmitter relating to an owned load facility.

**Distributor-Operator** - The organization operates a distribution system.

**Distributor-Owner** - The organization owns a distribution system.

**Electricity Storage Participant-MMP** - The organization is responsible for the financial settlements with respect to an electricity storage resource.

**Electricity Storage Participant-MMPT** - The organization is responsible for the financial settlement of metering data associated with a registered electricity storage facility.

**Electricity Storage Participant-Operator**- The organization operates an electricity storage facility.

**Electricity Storage Participant-Owner** - The organization owns an electricity storage facility.

**Electricity Storage Participant-RMP** - The organization submits dispatch or schedule data with respect to a registered electricity storage resource.

**Embedded Electricity Storage Facilities** - This participation is for organizations that do not require to be market participants, with embedded facilities (connected to a distribution system) greater than 10 MW.

**Embedded Generation Facilities** - This participation is for organizations that do not require to be market participants, with embedded facilities (connected to a distribution system) greater than 10 MW and that are not wind or solar generation.

**Embedded Load Facilities** - This participation is for organizations that do not require to be market participants, with embedded facilities (connected to a distribution system) that are required to register with the IESO.

**Energy Trader-Exporter** - The organization exports electricity out of Ontario.

**Energy Trader-Importer** - The organization imports electricity into Ontario.

**Generator-Metered Market Participant** - The organization is responsible for the financial settlement of metering data associated with a registered generation facility.

**Generator-Metered Market Participant Transmission Tariff** - The organization pays for one or more transmission services to a transmitter relating to an owned generation facility.

**Generator-Operator** - The organization operates a generation facility.

**Generator-Owner** - The organization owns a generation facility.

**Generator-Registered Market Participant** - The organization submits dispatch or schedule data with respect to a registered generation facility.

**Industrial Accelerator** - The organization is eligible to participate in the Industrial Accelerator Program (IAP) which is designed to assist eligible transmission-connected companies to fast track capital investment in major energy.

**Load-Metered Market Participant** - The organization is responsible for the financial settlement of metering data associated with a registered load facility.

**Load-Metered Market Participant Transmission Tariff** – The organization pays for one or more transmission services to a transmitter relating to an owned load facility.

**Load-Operator** - The organization operates a load facility.

**Load-Owner** - The organization owns a load facility.

**Load-Registered Market Participant** - The organization submits dispatch data with respect to a registered load facility that will be dispatchable.

**Meter Data Associate** - The organization will be authorized to be assigned by participants as a meter data associate to the participants' delivery points for the purpose of retrieving revenue meter data reports.

**Metering Service Provider** - The organization provides, installs, commissions, registers, maintains, repairs, replaces, inspects and tests metering installations.

**Multi-Distributor Customer Pay-for-Performance** - The organization participates in the Province-wide Pay-for-performance Conservation and Demand Management Program designed for Multi-Distributor Consumers.

**Operational Service Provider** - - No definition provided

**Program-Non-Specific** - The organization participates in an IESO program that is not listed.

**Regulation Service Provider** - The organization provides a regulation service to maintain balance between load and generation.

**Retailer** - The organization sells or offers to sell electricity to or for a consumer.

**Section** – a non-person *participant* contact entity such as a Service Desk, Control Room Operations area or Trading Floor that is registered with the IESO in the Registration system.

**Settlement Service Provider** - The organization provides a financial settlement service relating to metering data associated with a registered facility.

**Smart Metering Cost Recovery-Embedded Distributor** - The organization has a financial settlement with respect to the smart metering charge.

**Smart Metering Entity** - No definition provided

**Smart Metering Operating Service Provider** - The organization operates Ontario's Meter Data Management and Repository (MDM/R) system.

**Smart Submetering Provider** - The organization has a financial settlement with respect to Ontario Clean Energy Benefit Program Government electricity support program as a Smart Unit Sub-Metering Provider

**Transmission Rights** - The organization participates in the Transmission Rights market.

**Transmitter-Operator** - The organization operates a transmission system.

**Transmitter-Owner** - The organization owns a transmission system.

**- End of Section –**

# References

---

<b>Document Name</b>	<b>Doc ID</b>
Market Rules	MDP_RUL_0002
Market Manual 1: Market Entry, Maintenance & Exit, Part 1.1: Participant Authorization, Maintenance & Exit	MDP_PRO_0014
Market Manual 3: Metering, Part 3.1 Metering Service Provider (MSP) Registration, Revocation, and De-registration	MDP_PRO_0007
Market Manual 6: Participant Technical Reference Manual, Section 2.0: Participant Workstation, Network & Security	IMO_MAN_0024

– End of Document –