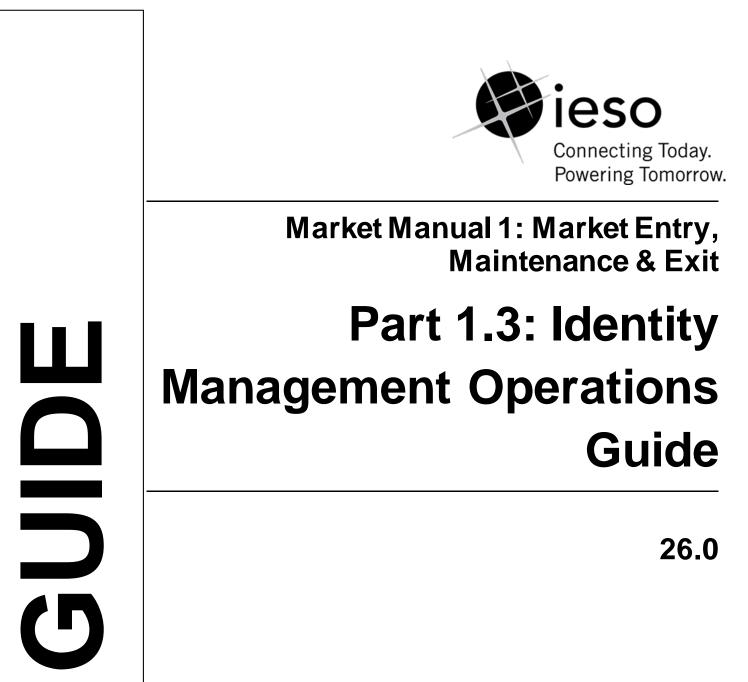
PUBLIC



This guide describes the processes for *Market Participant*s 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.

Public

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.

DocumentID	IMP_GDE_0088
Docum ent Nam e	Part 1.3: Identity Management Operations Guide
Issue	26.0
Reason for Issue	Revised for AODA requirements.
Effective Date	November 3, 2020

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 Accessibility for Ontarians with Disabilities Act	November 3, 2020		

Related Documents

Document ID	Document Title
IESO_GDE_0209	Portal Graphical User Interface User's Guide

Table of Contents

1. l	Introduction	1
1.1	Purpose	1
1.2	Scope	2
1.3	Who Should Use This Document	2
1.4	Overview	
	1.4.1 Provisioning, Identity Management, the <i>IESO</i> and the <i>Participant</i>	
	1.4.2 User Account Identity Credentials	
1.5	Assumptions and Limitations	
1.6	Conventions	
1.7	Document Organization	
1.8	Contact Information	5
2. F	Roles and Responsibilities of Identity Management Entities	6
3. I	dentity Trust Operational Model	8
3.1	IESO Trust Model	8
3.2	Identity Proofing	9
3.3	Rights Administrator Model	9
4. l	dentity Management Procedural Work Flows	10
4.1	Participant User Account Application Scenario	11
4.2	Participant User Account Change Scenario 1	12
4.3	Participant User Account Change Scenario 2	13
4.4	Participant User Account Deactivation Scenario	14
4.5	Participant User Account Recovery Scenario 1	15
4.6	Participant User Account Recovery Scenario 2	16
4.7	Participant Rights Administrator Enrolment Scenario	17
4.8	Participant Rights Administrator User Account Change Scenario 1	
4.9	Participant Rights Administrator User Account Change Scenario 2	19
4.10	O Participant Rights Administrator Role Termination Scenario	20
	1 Subscriber User Account Initialization	
4.12	2 Periodic Update of Subscriber User Account Password	22
5. F	Participant Primary Contact Operational Guidelines	24
5.1	Primary Contact Definition	
5.2	IESO Trust Model and Identity Credential Proofing 5.2.1 Participant Rights Administrator	
5.3	Appointing a Rights Administrator	

5.4	Process to Register a Rights Administrator and Request an Account and System Access	25
5.5	Requesting a Person's Rights Administrator Role Termination 5.5.1 Circumstances for Deactivation of IESO Systems Access and User Account	
5.6	Steps for Registering a Rights Administrator for Registration System Access and a User Account	25
6. F	Participant Rights Administrator Operational Guidelines	26
6.1	Rights Administrator Definition	
6.2	Instructions for Using the IESO Registration System	
6.3	IESO Trust Model and Guidelines for Proofing Credential Subscribers 6.3.1 When should the Identity of a Credential Subscriber Be Proofed	27
0.4	6.3.2 Process to Validate the Identity of the Credential Subscriber	
6.4	Guidelines for Form Storage, Protection, and Archival	
6.5	IESO Customer Relations Communications	
6.6	Guidelines for Distributing and Using Identity Credential Activation Data 6.6.1 IESO Personal User Account Credentials	
	6.6.2 User Account Activation - Temporary Password	
	6.6.3 Direct Delivery of Temporary password from an IT Operations Administrator	
6.7	Person ID Number	31
6.8	Basic Trouble Shooting	31
	C C	
	Credential Subscriber Operational Guidelines	
		32
7. C	Credential Subscriber Operational Guidelines	32 32 32
7. C 7.1	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing	32 32 32 33
7. C 7.1 7.2	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing 7.2.1 Participant Rights Administrator	32 32 33 33
7. 0 7.1 7.2 7.3	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing 7.2.1 Participant Rights Administrator Protection of Identity Credential Activation Data	32 32 33 33 33
7. C 7.1 7.2 7.3 7.4	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing 7.2.1 Participant Rights Administrator Protection of Identity Credential Activation Data Person ID Number	32 32 33 33 33 33
7. 0 7.1 7.2 7.3 7.4 7.5	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing 7.2.1 Participant Rights Administrator Protection of Identity Credential Activation Data Person ID Number Password Creation Guidelines.	32 32 33 33 33 33
 7.1 7.2 7.3 7.4 7.5 7.6 	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing 7.2.1 Participant Rights Administrator Protection of Identity Credential Activation Data Person ID Number Password Creation Guidelines Applying for an IESO Account	32 32 33 33 33 33 34 34 34
 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing	32 32 33 33 33 33 34 34 34 34 34 34
 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 	Credential Subscriber Operational Guidelines. Introduction. IESO Trust Model and Identity Credential Proofing. 7.2.1 Participant Rights Administrator. Protection of Identity Credential Activation Data. Person ID Number. Password Creation Guidelines. Applying for an IESO Account. IESO Systems Access Requests. IESO Account Deactivation. 7.8.1 Account Deactivation.	32 32 33 33 33 33 34 34 34 34 34 34
 7. C 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 	Credential Subscriber Operational Guidelines Introduction IESO Trust Model and Identity Credential Proofing	32 32 33 33 33 33 33 34 34 34 34 34 35 35
 7. C 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 	Credential Subscriber Operational Guidelines	
 7. C 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 8. U 	Credential Subscriber Operational Guidelines	32 32 33 33 33 33 33 34 34 34 35 35 35 36 37
 7. C 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 8. U 	Credential Subscriber Operational Guidelines	32 32 33 33 33 33 33 33 34 34 34 34 34 35 35 35 36 37 39

	Participations	.39
	Update Organization and Contacts	.41
	Rights Administrator	.50
	8.1.3 Online IESO Registration System Grant/Revoke Access Select System Access Request Type	
	Select Account Type	.53
	Search and Select a Registered Person	.54
	Register a New Person	.56
	Select Access Roles to be Granted	.58
	Select Access Roles to be Revoked	.60
	Machine Account Grant or Revoke Access Requests	.62
	New Machine Account	.64
	8.1.4 Registration System Mange Contact Information	.68
9. l	Use of Account Provisioning Tools	.71
9.1	Use of the Password Change & Reset Functions 9.1.1 Temporary Password Change	.71
	9.1.2 Password Self Recovery9.1.3 Navigating to the User Security Profile Page	.72 .83
10. I	9.1.2 Password Self Recovery	.72 .83 .89
10.1	9.1.2 Password Self Recovery 9.1.3 Navigating to the User Security Profile Page Browser Use	.72 .83 .89 .92 .92
10.1 10.2	 9.1.2 Password Self Recovery	.72 .83 .89 . 92 .92
10.1 10.2 11. 	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .92
10.1 10.2 11. 11.1	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .92 .94 .94
10.1 10.2 11. 11.1	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .94 .94 .94
10.1 10.2 11. 11.1	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .94 .94 .94 .−1 1
10.1 10.2 11. 11.1	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .94 .94 .94 .94 .94 1 1 1
10.1 10.2 11. 11.1	 9.1.2 Password Self Recovery	.72 .83 .89 .92 .92 .92 .94 .94 .94 1 .94 1 1

A.6 Participant User Account Recovery Scenario 2
A.7 Participant Rights Administrator Enrolment Scenario
A.8 Participant Rights Administrator User Account Change Scenario 1A-13
A.9 Participant Rights Administrator User Account Change Scenario 2 A-15
A.10 Participant Rights Administrator Role Termination Scenario
A.11 Subscriber User Account Initialization
A.12 Periodic Update of Subscriber User Account Password
A.13 Description of Changes
A.13.1 Credential Subscriber Information
A.13.2 Rights Administrator Information
Appendix B: Glossary of TermsB-1
Appendix C: List of ParticipationsC-1

List of Figures

FIGURE 4-2: PARTICIPANT USER ACCOUNT CHANGE SCENARIO 1	12
FIGURE 4-3: PARTICIPANT USER ACCOUNT CHANGE SCENARIO 2	13
FIGURE 4-4: PARTICIPANT USER ACCOUNT DEACTIVATION SCENARIO	14
FIGURE 4-5: PARTICIPANT USER ACCOUNT RECOVERY SCENARIO 1	15
FIGURE 4-6: PARTICIPANT USER ACCOUNT RECOVERY SCENARIO 2	16
FIGURE 4-7: PARTICIPANT RIGHTS ADMINISTRATOR ENROLMENT SCENARIO	17
FIGURE 4-8: PARTICIPANT RIGHTS ADMINISTRATOR ACCOUNT CHANGE SCENARIO 1	18
FIGURE 4-9: PARTICIPANT RIGHTS ADMINISTRATOR ACCOUNT CHANGE SCENARIO 2	19
FIGURE 4-10: PARTICIPANT RIGHTS ADMINISTRATOR ROLE TERMINATION SCENARIO	20
FIGURE 4-11: SUBSCRIBER ACCOUNT INITIALIZATION	
FIGURE 4-12: PERIODIC RENEWAL OF USER ACCOUNT PASSWORD	
FIGURE 8-1: REGISTRATION SYSTEM LINK IN IESO PORTAL	
FIGURE 8-2: REGISTRATION SYSTEM LOGIN SCREEN EXAMPLE	
FIGURE 8-3: ONLINE IESO APPLICANT REPRESENTATIVE - ACTIONS PAGE	
FIGURE 8-4: ONLINE IESO APPLICANT REPRESENTATIVE – SELECT PARTICIPATION TYPE PAGE	
FIGURE 8-5: ONLINE IESO APPLICANT REPRESENTATIVE – SELECT PARTICIPATION TYPE OPTION	
FIGURE 8-6: ONLINE IESO APPLICANT REPRESENTATIVE – MARKET PARTICIPATION TYPE	-
FIGURE 8-7: ONLINE IESO APPLICANT REPRESENTATIVE – MARKET PARTICIPATION CHOICES	40
FIGURE 8-8: ONLINE IESO APPLICANT REPRESENTATIVE – CHOOSING CAPACITY AUCTION MARKET	
PARTICIPATION FIGURE 8-9: ONLINE IESO APPLICANT REPRESENTATIVE – PARTICIPATION REQUIRED TASKS	
FIGURE 8-9: ONLINE IESO APPLICANT REPRESENTATIVE – PARTICIPATION REQUIRED TASKS	
FIGURE 8-11: ONLINE IESO APPLICANT REPRESENTATIVE OPDATE ORGANIZATION REQUEST TYPE	
FIGURE 8-12: ONLINE IESO APPLICANT REPRESENTATIVE OPDATE CONTACT ROLE(S) OPDATE TYPE	42
SEARCH	43
FIGURE 8-13: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) REGISTERED PERSON	
SEARCH RESULTS.	
FIGURE 8-14: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) REGISTERED PERSON	
SEARCH RESULTS 2	44
FIGURE 8-15: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) SELECTION FOR SELEC	
PERSON	
FIGURE 8-16: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) ADDED PERSON	46
FIGURE 8-17: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S), CONFIRMATION	47
FIGURE 8-18: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S), FINAL CONFIRMATION	N.47
FIGURE 8-19: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) SELECT CONTACT ROL	E
LIST	
FIGURE 8-20: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) - EXISTING CONTACTS	
FIGURE 8-21: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) - EXISTING PLUS NEW	
CONTACTS	49
FIGURE 8-22: ONLINE IESO APPLICANT REPRESENTATIVE UPDATE CONTACT ROLE(S) – PRIMARY	
CONFIRMATION	
FIGURE 8-23: ONLINE IESO REGISTRATION SYSTEM RIGHTS ADMINISTRATOR ACTIONS PAGE	
FIGURE 8-24: ONLINE IESO REGISTRATION SYSTEM NORMAL CONTACT ACTIONS PAGE	
FIGURE 8-25: CHOOSE AN ORGANIZATION PAGE	
FIGURE 8-26: SELECT SYSTEM ACCESS REQUEST TYPE PAGE	
FIGURE 8-27: SELECT ACCOUNT TYPE PAGE - GRANT	
FIGURE 8-28: SEARCH FOR A REGISTERED PERSON PAGE - GRANT	54

FIGURE 8-29: SELECT A REGISTERED PERSON PAGE - GRANT	.55
FIGURE 8-30: REGISTER A NEW PERSON PAGE - GRANT	
FIGURE 8-31: CONFIRM NEW PERSON REGISTRATION PAGE - GRANT	.57
FIGURE 8-32: SELECT ACCESS ROLES TO BE GRANTED PAGE	.58
FIGURE 8-33: CONFIRM ACCESS ROLE(S) TO BE GRANTED PAGE	.59
FIGURE 8-34: SELECT ACCESS ROLES TO BE REVOKED PAGE	.60
FIGURE 8-35: CONFIRM ACCESS ROLE(S) TO BE REVOKED PAGE	.61
FIGURE 8-36: SELECT MACHINE ACCOUNT PAGE - GRANT	.62
FIGURE 8-37: SELECT MACHINE ACCOUNT PAGE - REVOKE	
FIGURE 8-38: CONFIRM EXISTING MACHINE ACCOUNT PAGE - GRANT	
FIGURE 8-39: CREATE MACHINE ACCOUNT FOR ACCESS ROLE GRANT PAGE	.65
FIGURE 8-40: SELECT ACCESS ROLE(S) TO BE GRANTED - MACHINE ACCOUNT PAGE	
FIGURE 8-41 CONFIRM ACCESS ROLE(S) TO BE GRANTED – MACHINE ACCOUNT PAGE	
FIGURE 8-42 CHOOSE AN ACTION PAGE	
FIGURE 8-43 UPDATE PERSON INFORMATION PAGE	
FIGURE 8-43 CONFIRM PERSON INFORMATION PAGE	
FIGURE 9-1: PORTAL / IDENTITY MANAGEMENT LOGIN – USER ACCOUNT NAME ENTRY	
FIGURE 9-2: PORTAL / IDENTITY MANAGEMENT LOGIN – PASSWORD ENTRY	
FIGURE 9-3: PORTAL / IDENTITY MANAGEMENT LOGIN – PASSWORD RESET	.74
FIGURE 9-4: PORTAL/IDENTITY MANAGEMENT LOGIN – USER ACCOUNT NAME AND/OR PASSWORD ERRO	
MESSAGE	
FIGURE 9-5: PORTAL / IDENTITY MANAGEMENT LOGIN – PASSWORD RESET	
FIGURE 9-6: PORTALIDENTITY MANAGEMENT LOGIN PAGE - CHANGE PASSWORD - MISMATCH ERROR	
FIGURE 9-7: PORTALIDENTITY MANAGEMENT LOGIN PAGE - CHANGE PASSWORD - OLD PASSWORD ERROF	78
FIGURE 9-8: PORTALIDENTITY MANAGEMENT LOGIN PAGE - CHANGE PASSWORD NOTIFICATION EMAIL	-
FIGURE 9-9: PORTALIDENTITY MANAGEMENT LOGIN PAGE – NEW ACCOUNT SECURITY PROFILE	.80
FIGURE 9-10: PORTAL IDENTITY MANAGEMENT LOGIN PAGE – LOGIN TECHNICAL ERROR	
FIGURE 9-11: SECURITY PROFILE – CHOOSING A SECURITY IMAGE AND PHRASE	
FIGURE 9-12: SECURITY PROFILE - CHOOSING SECURITY QUESTIONS AND INPUTTING ANSWERS	
FIGURE 9-13: PORTAL IDENTITY MANAGEMENT LOGIN PAGE - FORGOT PASSWORD OPTION	-
FIGURE 9-14: USER ACCOUNT PASSWORD RESET SECURITY QUESTION EXAMPLE	
FIGURE 9-15: USER ACCOUNT PASSWORD RESET - INVALID ANSWER PROVIDED	
FIGURE 9-16 USER ACCOUNT PASSWORD RESET – ACCOUNT LOCKED	
FIGURE 9-17: USER ACCOUNT PASSWORD - RESET YOUR PASSWORD – NEW PASSWORD ENTRY	
FIGURE 9-18: USER ACCOUNT PASSWORD RESET STEP 3 OF 4 – INVALID NEW PASSWORD ENTRY	
FIGURE 9-19: USER ACCOUNT LOGIN – WELCOME TO YOUR PORTAL LOGIN SCREEN DISPLAYED	
FIGURE 9-20: TYPICAL PORTAL HOME PAGE WITH SECURITY PROFILE TAB	
FIGURE 9-21: PORTAL SECURITY PROFILE PAGE - PERSONAL IMAGE AND PHRASE PREFERENCES	
FIGURE 9-22: PORTAL SECURITY PROFILE PAGE – SECURITY QUESTIONS	
FIGURE 9-23: PORTAL SECURITY PROFILE PAGE – CHANGE YOUR PASSWORD	
FIGURE 11-1: MARKET INFORMATION MANAGEMENT APPLICATION INTERFACE (WEB SERVICES) DOWNLOA	
	.94

List of Tables

TABLE 2-1: IDENTITY MANAGEMENT ROLES AND RESPONSIBILITIES	6
TABLE 4-1: LEGEND FOR WORK FLOW DIAGRAMS	10
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–4
TABLE A-4: PARTICIPANT USER ACCOUNT DEACTIVATION SCENARIO TASK DETAILS	A–5
TABLE A-5: PARTICIPANT USER ACCOUNT RECOVERY SCENARIO 1 TASK DETAILS	A–7
TABLE A-6: ACCOUNT RECOVERY SCENARIO 2 TASK DETAILS	A–9
TABLE A-7: RIGHTS ADMINISTRATOR ENROLMENT SCENARIO TASK DETAILS	
TABLE A-8: RIGHTS ADMINISTRATOR CHANGE SCENARIO 1 TASK DETAILS	A–13
TABLE A-9: PARTICIPANT RIGHTS ADMINISTRATOR ACCOUNT CHANGE SCENARIO 2 TASK DETAILS	A–15
TABLE A-10: PARTICIPANT RIGHTS ADMINISTRATOR ROLE TERMINATION SCENARIO TASK DETAILS	A–17
TABLE A-11: CREDENTIAL SUBSCRIBER, ACCOUNT INITIALIZATION TASK DETAILS	A–19
TABLE A-12: UPDATE OF ACCOUNT PASSWORDS	A–21

Table of Changes

Reference (Section and Paragraph)	Description of Change
All sections	Updated all pictures to add alternate text information, removed extraneous spaces, fixed grammatical contexts, shortened headings that were too long.

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 *IESO* Portal for;
 - Participating in transmission rights auctions;
 - Accessing *settlement* and *invoice* data;
 - Accessing various Collaboration communities such as the SOE LDC Extranet
- 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 Outage Management system and
- 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, 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. User Account / Password) for authentication and authorization purposes.

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 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 <u>"Identity Trust Operational Model"</u> 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. This shall mean that at most, a user will receive one personal User Account where feasible.

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 User IDs can be used to establish authentication, authorization, and integrity.

Before receiving 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 and password will be issued upon authorized registration for access to the appropriate systems and applications. A temporary password shall be supplied in conjunction with the User Account credential for a User account for the *IESO* Portal, Report site, Energy Market Interface, Outage Management system, Online IESO system for, Registration and other application purposes or where applicable Web Services. The temporary password as indicated above needs to be replaced with one of their choosing by the end user by initially logging into the IESO Portal. The temporary password will expire automatically after approximately two weeks during which time the end user can update it via Portal login. After the temporary password.

Upon initial login to the Portal, the user shall be required to reset their password using an online web provisioning process and to select a security image and phrase as well as choose 5 security questions and answers. The chosen security image and phrase will be presented to the user on each login to the Portal, Energy Market Interface and Outage Management system to provide confidence that the authentic IESO system is being connected and logged in to. The 5 security questions and answers selected by the user shall be usable 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 security questions and answers will also be used to permit the users to reset their own passwords if forgotten during login. The Portal's reset password 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 Portal, be able to change their password as well on the 'Security Profile' web page in the Portal. The link for the Security Profile web page is available within the Portal's community pages.

A person's user account is common to the Portal, Online IESO, Energy Market Interface, Outage Management System and Reports site. This means the same account UserID and enduring password is used for access to each system.

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 or via telephone, mail or courier to the numbers and addresses given on the *IESO*'s Web site (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

Title	Description	
IESO		
IESO ITOPS Customer Support	<i>IESO</i> ITOPS Customer Support is responsible for managing credential issuance, user name changes and credential deactivation requests using appropriate tools and procedures, (i.e. for processing requests to <u><i>IESO</i></u> systems administrators).	
IESO Customer Relations	<i>IESO</i> Customer Relations is responsible for managing credential recovery requests using appropriate tools and procedures.	
Participant		
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 AppendixC.	
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 IESO 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 IESO 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 IESO 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 as signed to an application. 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.	
General Terms		
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 the new registration processes, the IESO is enabling business process automation and removing a great deal of administrative burden for the participants. To do so, it needed to establish a new and simpler trust model entirely divorced from the PKI legacy and streamlined to be automated and supported by the BPMS tools.

In the new trust model for management of access rights, Authorized Representatives are 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 going forward. Its 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.

The Rights Administrator is responsible for handling all user account requests other than Primary Contacts and Authorized Representatives. This includes the User Account issuance and system access role requests, user credential changes and deactivation requests and User Account password reset requests.

– 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.

Legend	Description
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.

Table 4-1: Legend for Work Flow Diagrams

4.1 Participant User Account Application Scenario

In this scenario, a *participant* employee or contractor applies for a user account and participant contact roles and/or system access roles / permissions via the *participant* Rights Administrator.

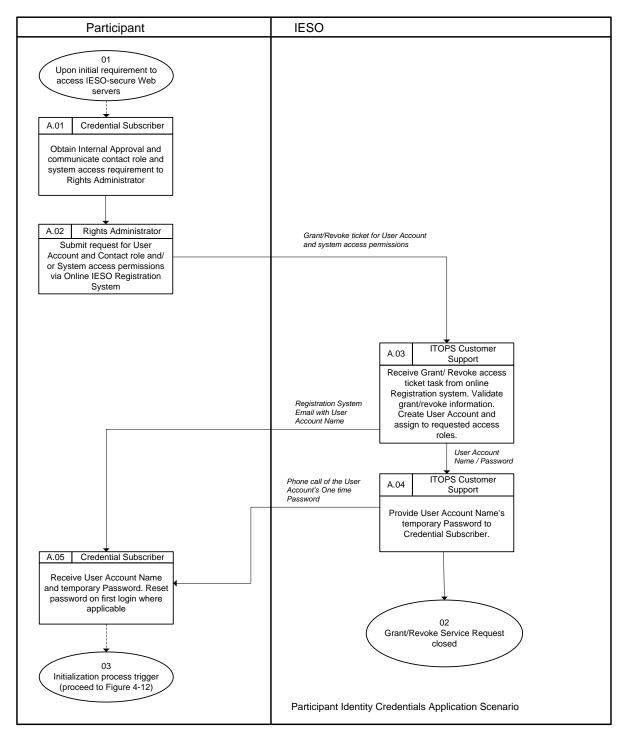


Figure 4-1: Participant User Account Application Scenario

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 a Rights Administrator.

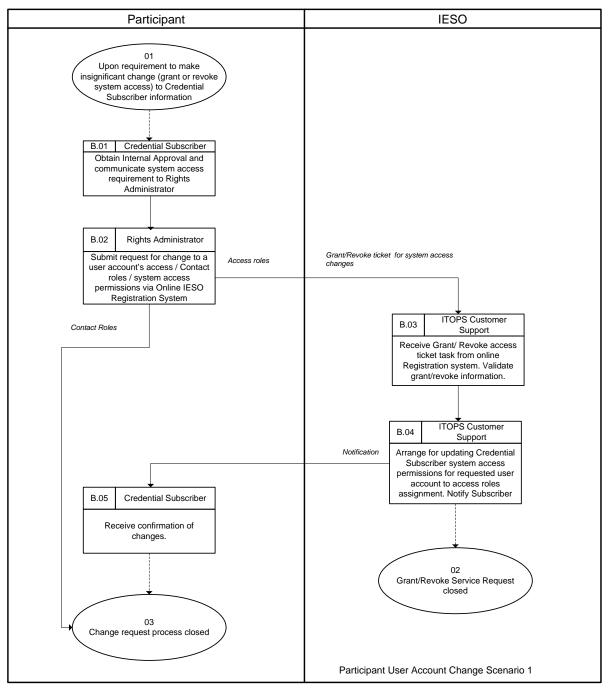
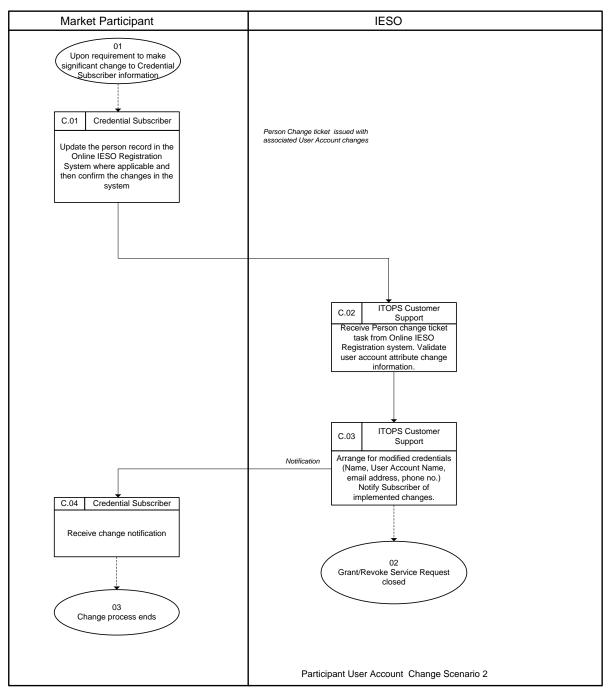
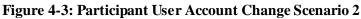


Figure 4-2: Participant User Account Change Scenario 1

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.





4.4 Participant User Account 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 deactivation as it is no longer required and a *participant* Rights Administrator submits that request.

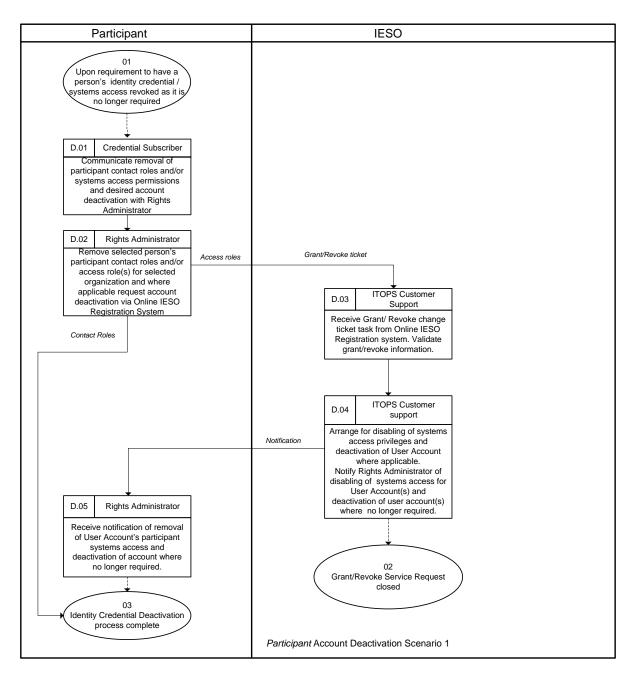


Figure 4-4: Participant User Account Deactivation Scenario

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.

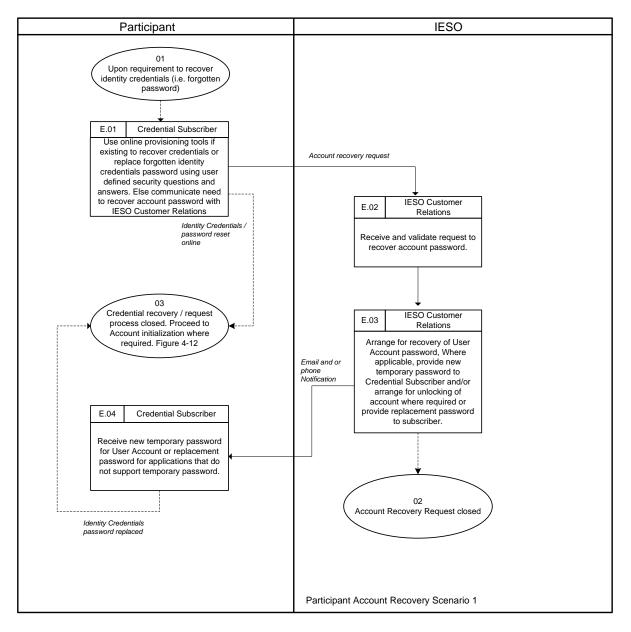


Figure 4-5: Participant User Account Recovery Scenario 1

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.

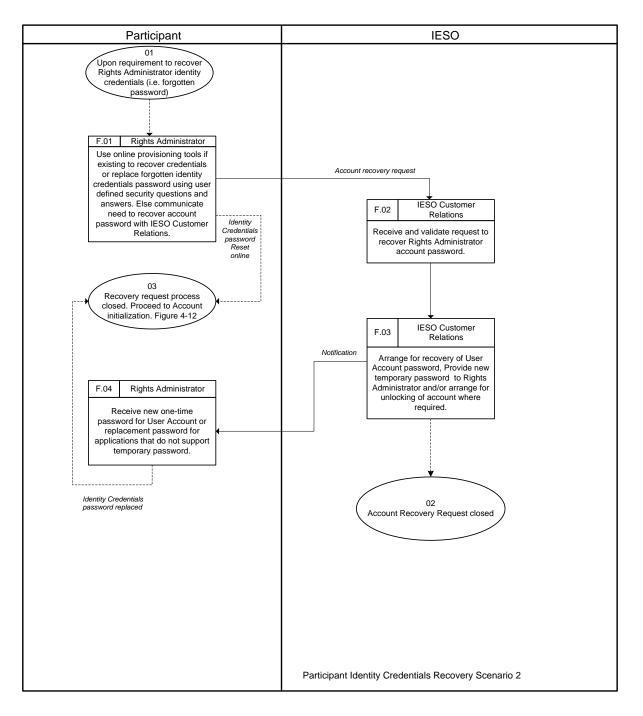


Figure 4-6: Participant User Account Recovery Scenario 2

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.

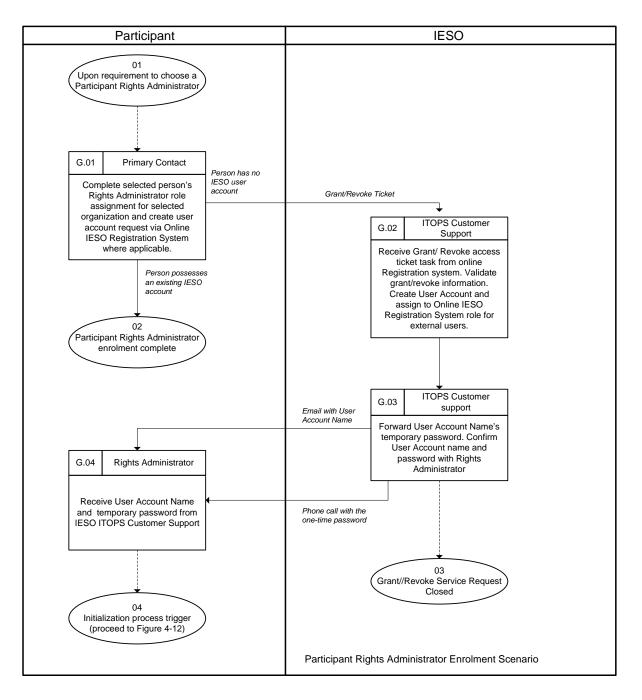


Figure 4-7: Participant Rights Administrator Enrolment Scenario

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.

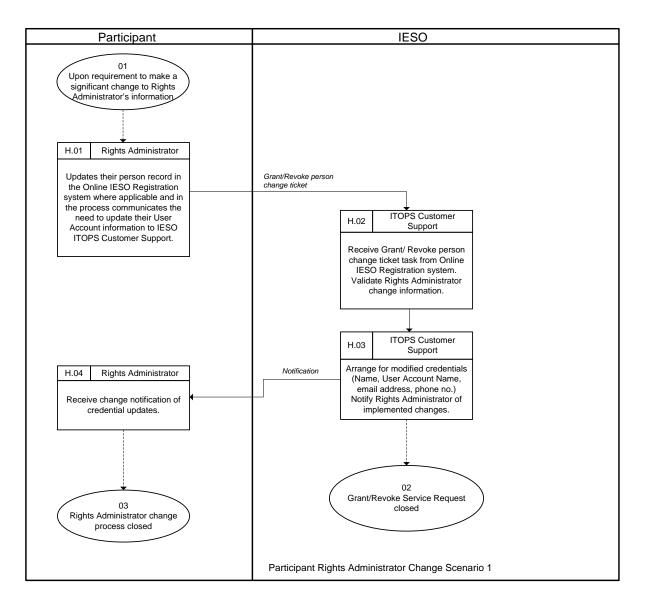
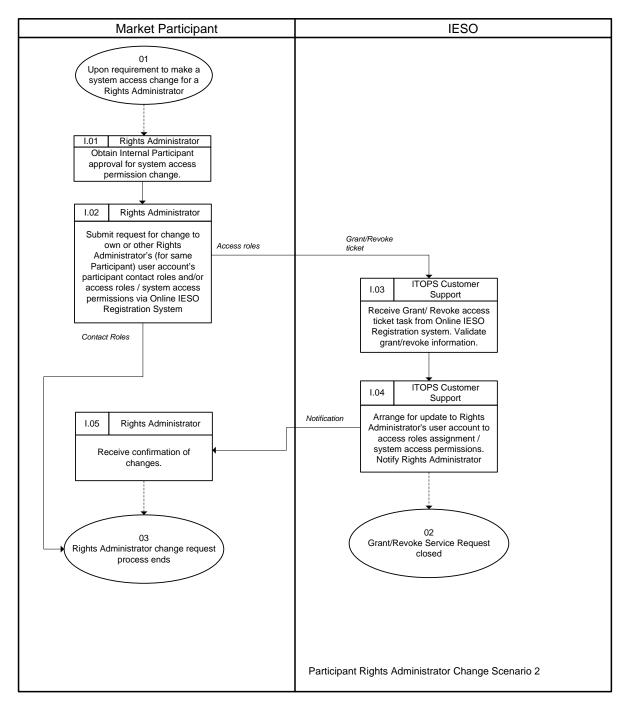
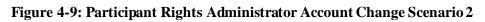


Figure 4-8: Participant Rights Administrator Account Change Scenario 1

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.





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.

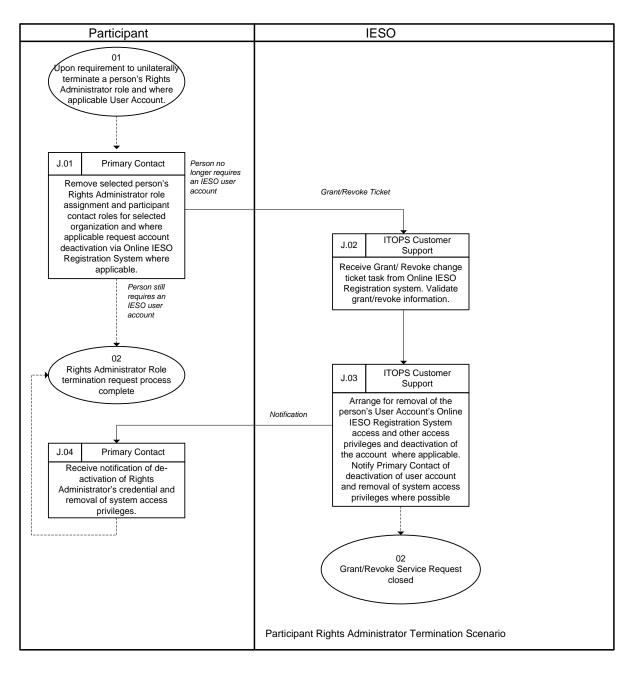
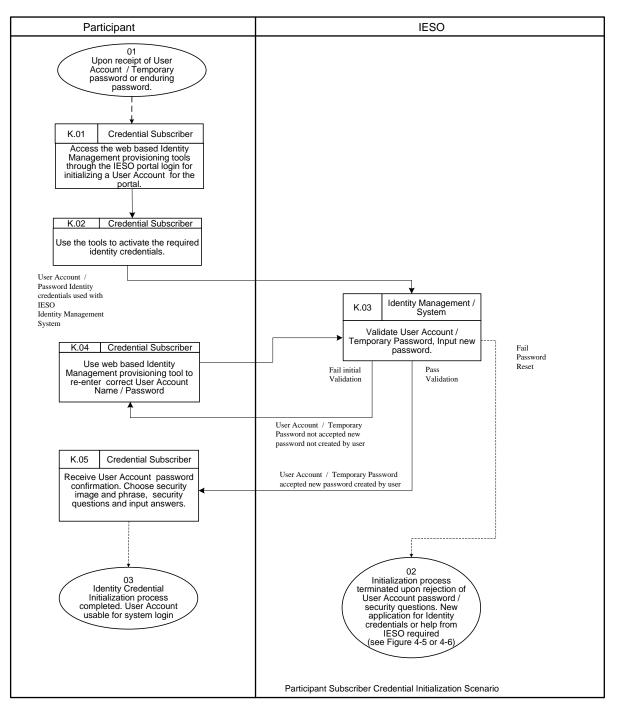


Figure 4-10: Participant Rights Administrator Role Termination Scenario

4.11 Subscriber User Account Initialization

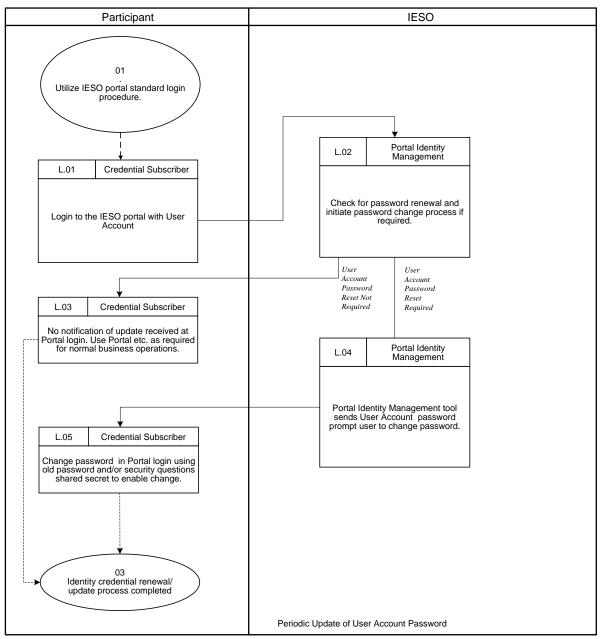
The following diagram represents the process by which an Authorized Representative, Primary Contact, Individual Subscriber, Application Subscriber or Rights Administrator, etc. can activate their Portal, Online IESO, Report Site, Energy Market Interface, Outage Management system, User Account/Password.

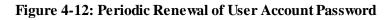




4.12 Periodic Update of Subscriber User Account Password

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 updated when logging in to the IESO Portal. Password reset involves password changes to a User Account. After password reset has been completed successfully the same account may be used to login to the Portal, Report Site, Energy Market Interface site, Outage Management site, Online IESO Registration system, etc. where granted access privileges permit.





- 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 <u>"Appointing a Rights Administrator"</u> 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 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 must use the *IESO* supplied temporary password for initial login to the identity management system used with the Portal. The temporary password for a User Account credential must <u>first be used</u> to login to the Portal and changed on the initial attempted login. Using the temporary password directly against the Report site, or Online IESO system etc. will work but will cease to do so after a few weeks and then the user will need to communicate to the IESO for a password reset.

The same is essentially the same now for the Credential Subscriber (custodian) who applies for and receives a User Account credential used with the MIM Web Services (i.e. machine account). She or he will securely receive a temporary password from the IESO. The custodian will then need to login to the Portal and in the process of doing so reset the password to one of his/her own choosing and set up the associated security questions and answers. However, the machine account will have no market application access permissions in the Portal and the custodian can logout. The account can then be used with the MIM Web Services. The custodian can periodically (on a schedule of his / her own choosing), change the password and security questions and answers for the machine account by logging into the Portal and access the 'Security Profile' page in the Welcome community to do so (see procedure below).

6.6.1 IESO Personal User Account Credentials

Any User Account credential for an IESO personal user account ID shall 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. It the user's last name is greater than 7 characters, then it will be truncated at the 7th 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 7th and 8th 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
- 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 *IESO* Registration system will forward a grant/revoke ticket to those responsible in IESO IT Operations for creating the account or granting system access privileges. IT Operations will create the User Account and the Registration system will email the account User Name 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 *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 IESO IT Operations may contact the Rights

Administrator or Credential Subscriber directly, to aid in the delivery of the User Account to the Credential Subscriber by obtaining the correct email.

6.6.2 User Account Activation - Temporary Password

Any User Account credential for an *IESO* user or machine account used with the Portal, Report Site, Energy Market Interface, Outage Management system, Online IESO Registration system, or any Web Service where applicable shall have a temporary password (or one that is reset at the valid request of a user) generated by *IESO* IT Operations under 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)

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 five passwords.

Only one method will be used for the delivery of the temporary /reset password to the Credential Subscriber as defined below. Throughout the entire process, knowledge of the password must be kept solely between an *IESO* IT Operations administrator and the Credential Subscriber. Once the User Account ID and temporary password have both been received by the Credential Subscriber, he/she can login to the Portal / Identity Management system with that User Account and one-time password and reset the password as required. The Credential Subscriber should also choose a security image and phrase and five security questions and input appropriate answers for password self-recovery and extra authentication purposes as well.

6.6.3 Direct Delivery of Temporary password from an IT Operations Administrator

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

• By Phone

The IT Operations Administrator 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.

It shall be the responsibility of each person to maintain correct phone and email information in their person record. The 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* Portal, Online IESO, Energy Market Interface, Outage Management system, IESO Reports Site or other 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 authentifiers, 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 three distinguishing features:
 - Upper-case
 - Lower-case
 - Special character (punctuation and other symbols). Do not use ampersand &, backslash \, less than symbol <, greater than symbol >, single quote ', double quote "
- Recommended to use numbers as well
- Includes no spaces

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 within their Organization. Once the Initial Issuance process has been competed the Credential Subscriber will receive an email of the User Account name (i.e. UserID) created and a User Account temporary password directly from the IESO IT Operations administrator by phone. 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 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 for instructions on how to use a User Account's 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 along with the appropriate internal *participant* approval for such. The Rights Administrator 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 a workflow ticket will be created where required by the Registration system to the IESO IT Operations Administrator to add or remove the user's account in the appropriate system access role groups and notification of the enrolment change will be sent back to the Rights Administrator 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* Portal, Reports site, Online IESO Registration system, Prudential system, Energy Market Interface, Outage Management System or MIM API service and the user account attributes have become inaccurate (e.g. name change, email address change, phone number change or system access requirements)

7.10 Account Recovery

All requests for User Account 'forgotten password' reset that the users (or custodian for machine accounts) cannot reset themselves with their self-chosen security questions and answers) 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. 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 the User Account and password is communicated to the Credential Subscriber, the user can log on to the appropriate 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 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 Registration System

All *participant* Organization Applicant Representatives, Contacts and Rights Administrators can access the Online IESO Registration system by Accessing the IESO Portal (either Sandbox or Production) and click on the IESO Registration link in the Portal "IESO Related Links" as shown in Figure 8-1

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.

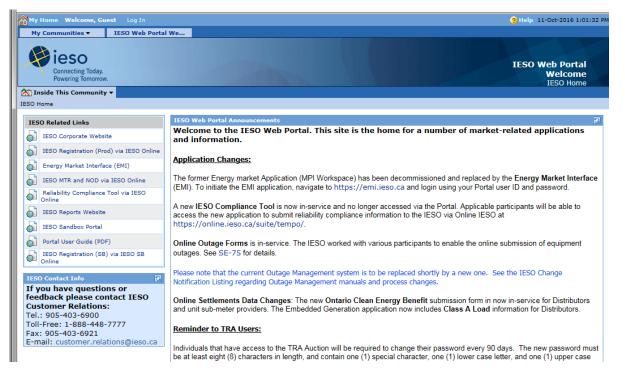


FIGURE 8-1: Registration System Link in IESO Portal

The link in each Portal will navigate the *participant* user to the associated Sandbox or Production Online IESO Registration system login screen in a new browser tab as shown in the example in Figure 8-2

Username	
Password	
Remember me on this con	nouter
Forgot Password	Sign In
Attention to Participants: Thi operated by the IESO, and al governed by the Market Rule you have received a unique a and Password from the IESO agree to maintain their confin agree that you are exclusivel and any activity on this syste of your User Account and Pas of any unauthorized use of yi you agree to immediately no liable for any loss or damage	s system is owned and I use of this system is s. As a registered Participant, and confidential User Account to access this system and you dentiality. You specifically y responsible for all access to m that occurs through the use usword. If you become aware our User Account or Password, tify the IESO. The IESO is not arising from any unauthorized and assword. If you do

Figure 8-2: Registration System Login Screen Example

The "Forgot password link will navigate the user to the corresponding Portal login 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 matching Portal and Online IESO Registration systems in each environment but the same account/password is not used between Production and Sandbox.

8.1.2 Online IESO Registration System Actions

Applicant Representative

Successful login to the Online IESO Registration system by an Applicant Representative will take them to an 'Actions' page as shown in Figure 8-3.

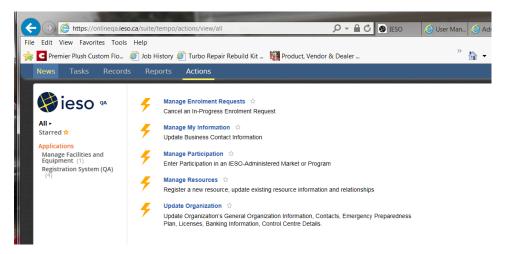
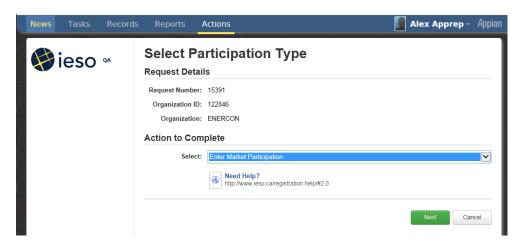


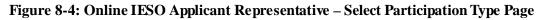
Figure 8-3: Online IESO Applicant Representative - Actions Page

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.





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.

Enter Market Participation	
Enter Program Participation	
Enter Service Provider 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.

News	Tasks	Records	Reports	Actions		Alex Apprep -	Appian
*	ieso	QA	Market	arket participation	ation for which authorization will be requested		
					t Participation		
			Market Parti Market*		pe		Y
						Ne	ext

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

Select a Value	
Senerator	
oad	
nergy Trader	
ransmitter	
ransmission Rights	
letailer	
apacity Auction	
lectricity Storage Participant	
apacity Market Participation	

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

Request Details	
Request Number: 19366	
Organization ID:	
Organization:	
Request Type: Enter Market Participation	
Market Participation Type	
markeer arciepation type	
tarket *	
Aarket * Capacity Auction Gapacity Auction Gov organization is eligible to participate in the Capacity Auction.	

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

ted pelow are the tasks that must be completed by the requesting organization for this participation type.	
equest Details	
Request Number: 19366	
Organization ID:	
Organization:	
Request Type: Enter Market Participation	
uticipation Type: Capacity Auction	
equired Tasks	
Confirm Connectivity to IESO Information System(s)	
issign Contact Role(s)	
Need Help? Ntp://www.ieso.ca/registration.help/#2.4	

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.

News Tasks Record	ds Reports Actions	🚺 Alex Apprep - Appi
💱 ieso 🏾	Select 'Update Organization' Request Details	' Request Type
	Organization ID: 122846 Organization: ENERCON Select Request Type	
	Select: Update Contact Role(s) Update Section Update Organization Information Update Licence Update Emergency Preparedness Plan Manage Control Centres Update Facility Contact	
		Next Cancel

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

News Tasks Record	s Reports A	Actions	📕 Alex Apprep - Appian
💱 ieso 🛚	Select an Request Detail	Update Type	
	Organization ID: Organization: Request Type:		By Person By Role By Section

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.

News Tasks Record	s Reports /	Actions	Alex Apprep - Appiar
😻 ieso 🏻	Search fo	or a Registered Person	
	Organization ID:		
	Organization: Request Type:	Update Contact Role(s) by Person	
	Search for a R	egistered Person	
		Search for the registered person using the following search fields. E accurate results. At least one field must be filled in for the search. If	
	Person ID	the person can then be registered.	
	Last Name		
	First Name	Need Help?	
		http://www.ieso.ca/registration.help/#1.31	
			Search for Person

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.

News Tasks Records	Re	eports Actions	Wo	orking		🚺 Alex Apprep - Appian
🏈 ieso 🛚	Requ Org (R	lect Registere uest Details panization ID: 122848 Organization: ENERCON equest Type: Update Contact rch Results				
		Person ID	Last Name	First Name	Preferred Name	Middle Name
		507488	Smith	Bob		
		507522	Smitham	Thais		
		507523	Smith	David L.		
		507524	Smith	Gordon		
		507525	Smith	Linda		
		507526	Smith	Mary Ann		
		507527	Smith	Scott		
		507528	Smith	Velma		
		507529	Smith	Wade		
		507530	Smit	Joshua		
		Person ID Last Name First Name Need He		your search in the fields below or cli	ck 'Register New Person'.	Register New Person Cancel

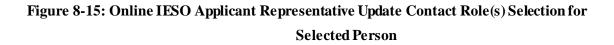
Figure 8-13: Online IESO Applicant Representative Update Contact Role(s) Registered Person Search Results

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".

News Tasks Record	ls Re	eports Ac	tions				Alex Apprep -	Appian
News Tasks Record		lect Reg uest Details		ed Person				
	R	ganization ID: 1 Organization: E Request Type: U TCh Results	NERCON	act Role(s) by Person				
		Person ID		Last Name	First Name	Preferred Name	Middle Name	
		507445		Smith	Bob			
		507486		Smith	Bob			
		507488		Smith	Bob			
		Person ID	smith bob			w or click 'Register New Person'.	Register New Person) Ca	ncel

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.

News Tasks Records	5 Re	eports Actions	5	We	orking				Alex App	r ep - <i>A</i> ppia
🚱 ieso 🛚	-	date Conta	act Ro	le(s)						
		anization ID: 122846								
		Organization: ENERC equest Type: Update		(s) by Person						
		erson Name: Bob Sm								
	Avai	lable/Removed (Contact R	Role(s)						
				ole(s)' to add selected cor both 'Dispatch Data Subn	ntact role(s). nitter' role and 'Dispatch Da	ata Viewer' at the same	time			
		Contact Role Name	Description	n			Min. Required	No. Of Existing	Max. Permitted	Status
		18 Month and Long- Term Assessments	Person resp reliability as	ponsible for data submissi ssessments for your organ	ons for the 18-Month Outlo ization.	ioks and longer-term	o	o	-	
		Authorized Representative	Person resp assigns Prin	ponsible for contractually i mary Contacts.	binding your organization w	ith the IESO. This role	1	o	-	
		Bids and Offers	Person or S for your org	Section responsible for sul anization.	bmitting and/or changing re	al-time bids or offers	0	1		
		Compliance and Market Surveillance	Person resp administere	ponsible for discussing pa ed markets for your organi	rticipant conduct and activi zation.	ties within the IESO-	0	o	-	
		Dispatch Data Submitter	Person or S for your org	Section responsible for sul anization.	omitting and/or changing re	al-time bids or offers	1	2		
		Dispatch Data Viewer	Person or S your organi	Section responsible for vie zation.	wing and/or changing real-	time bids or offers for	1	o		
		Emergency Preparedness Plan	Person resp your organi	ponsible for submitting an zation.	d updating the Emergency	Preparedness Plan for	1	1		
		Equipment Registration Specialist	Person resp	ponsible for registering eq	uipment/resource for your	organization.	1	10	-	
	Information Technology		Person or S technology	Section responsible for con services, projects and cha	mmunicating with the IESO anges for your organization	0	1			
		Invoicing and Banking	Person resp for your org	ponsible for submitting an anization.	1					
	Market Participant Compliance Contact		Person resp Program for Certification compliance	ponsible for reliability com r your organization. This in ns, periodic data submittal e, submitting Self-Reports	pliance under the Ontario F ncludes preparing and subr s and data requests. In case and providing associated n	o	o			
		Market Participant Escalation Contact	Person resp are missed This person Participant	ponsible for reporting relia) under the Ontario Reliab n is preferably of higher au Compliance Contact.	bility compliance on escala ility Compliance Program f thority than the person des	0	o			
		MMP Meter Trouble Report	Person resp receiving M	ponsible for monitoring Me leter Trouble Reports stat	eter Trouble Reports, addin us notifications.	1	1	-		
		Notice of Disagreement	Person resp for your org	Person responsible for submitting Notices of Disagreement for settlement statements 1 1						
		Revenue Metering	Person resp flight data s Contact for Reports for	ponsible for viewing the m submitted during a meter r a transmitter organization transmission delivery poi	aster data for registered m egistration request. The Re is responsible for approvir nts.	eter installations and in- evenue Metering ng Site Registration	1	1		
		Settlements			ons relating to settlement s		o	o	-	
		🕘 1-16 of 18 🕟 🛞								
	Exis	ting/Added Cont	tact Role((S)						
		Click 'R Role(s)'	emove Conta	ct Role(s)' to remove sele	cted contact role(s). To re	move all contact role(s),	select the top	o left check box and	then click 'Rem	ove Contact
		Contact Role Name		Description	Min. Required	No. Of Existing		Max. Permitted	SI	tatus
					No items avai	lable				
			eed Help? ttp://www.ieso.	ca/registration.help/#1.25						
						Done	Cancel	Add Contact Role(s)	Remove Co	ontact Role(s)



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

ews Tasks Records	; R€	ports Actions	5				Alex App	rep - Ap		
🖗 ieso 🛚		date Conta	act Role(s)							
		anization ID: 122846	1							
	C	Organization: ENERG	CON							
			Contact Role(s) by Person							
	Person Name: Bob Smith Available/Removed Contact Role(s)									
	Avai		dd Contact Role(s) to add selected contact role(s).							
		Contact Role		Mi	_	No. Of	Max.			
		Name	Description	Re	quired	Existing		Status		
		18 Month and Long- Term Assessments	Person responsible for data submissions for the 18-Month Outlooks and long term reliability assessments for your organization.			0	-			
		Authorized Representative	Person responsible for contractually binding your organization with the IESO role assigns Primary Contacts.	This 1		0				
		Bids and Offers	Person or Section responsible for submitting and/or changing real-time bids of offers for your organization.			1	-			
		Compliance and Market Surveillance	Person responsible for discussing participant conduct and activities within the IESO-administered markets for your organization.	• 0		0				
		Dispatch Data Submitter	Person or Section responsible for submitting and/or changing real-time bids or offers for your organization.			2				
		Dispatch Data Viewer	Person or Section responsible for viewing and/or changing real-time bids or of for your organization.			0				
		Emergency Preparedness Plan	Person responsible for submitting and updating the Emergency Preparednes for your organization.			1				
		Equipment Registration Specialist	Person responsible for registering equipment/resource for your organization.	1		10	-			
		Information Technology	Person or Section responsible for communicating with the IESO about inform technology services, projects and changes for your organization.	ation 0		1				
		Invoicing and Banking	Person responsible for submitting and maintaining, or approving banking information for your organization.	1		1	-			
		Market Participant Compliance Contact	Person responsible for reliability compliance under the Ontario Reliability Compliance Program for your organization. This includes preparing and sub- Self-Certifications, periodic data submittals and data requests. In case of pot non-compliance, submitting Self-Reports and providing associated mitigation	nitting 0 ential 0 plans.		0				
		Market Participant Escalation Contact	Person responsible for reporting reliability compliance on escalated matters (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.	due 0		0	-			
		MMP Meter Trouble Report	Person responsible for monitoring Meter Trouble Reports, adding comments, receiving Meter Trouble Reports status notifications.	and 1		1	-			
		Notice of Disagreement	Person responsible for submitting Notices of Disagreement for settlement statements for your organization.	1		1	-			
		Revenue Metering	Person responsible for viewing the master data for registered meter installati and in-flight data submitted during a meter registration request. The Revenue Metering Contact for a transmitter organization is responsible for approving S Registration Reports for transmission delivery points.	ons 8 1 Site 1		1				
	8.6	0 1-15 of 15 🕟 🖗								
	Exis	ting/Added Con	tact Role(s)							
		Click 'R Contac	lemove Contact $Role(s)$ ' to remove selected contact $role(s)$. To remove all control $Role(s)$.	tact role(s), s	elect the to	p left check	box and then click	'Remove		
		Contact Role Name		Min. Required	No. Exis	Of	Max. Permitted	Status		
		Settlements	Person responsible for issues/questions relating to settlement statements for your organization.	0	1		-			
		3 h	leed Help? ttp://www.ieso.ca/registration.help/#1.25							
			Party -							
			Done	Cance	Add	i Contact Ro	Remove C	ontact Role(s)		

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.

News Tasks Records	Reports A	ctions			Alex Appre	∍ p - Appian					
🟈 ieso 🛚	Confirm C Request Detail	contact Role(s) s									
	Organization ID:										
	Organization:	ENERCON									
	Request Type: Update Contact Role(s) by Person										
	Person Name:	Bob Smith									
	Contact Role(s) to be Added										
	Contact Role Name	Description	Min. Required	No. of Existing	Max. Permitted	Status					
	Settlements	Person responsible for issues/questions relating to settlement statements for your organization.	0	1	-						
	Contact Role(s) Summary										
		This is the list of contact role(s) the person/section will have after you click 'Confirm'									
	Contact Role Name	Description	Min. Required	No. of Existing	Max. Permitted	Status					
	Settlements	Person responsible for issues/questions relating to settlement statements for your organization.	0	1	-						
					Confirm	Cancel					

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.

	s Reports /	Actions				Alex App	orep - Appian					
🏈 ieso 🛚	Confirm (Request Detai		Role(s)									
	Organization: Request Type: Person Name:	Organization ID: 122846 Organization: ENERCON Request Type: Update Contact Role(s) by Person Person Name: Bob Smith										
	Contact Role(s	Contact Role(s) to be Added										
	Contact Role Name	Description		Min. Required	No. of Existing	Max. Permitted	Status					
	Settlements	Person respo your organiza	onsible for issues/questions relating to settlement statements for ation.	o	1	-						
	Contact Role(s) Summary											
		This is the list o	f contact role(s) the person/section will have after you click 'Confirm	<i>.</i>								
	Contact Role Name	Descriptior	Are you sure you would like to assign the listed	Min. Required	No. of Existing	Max. Permitted	Status					
	Settlements	Person resp your organiz	contact role(s) to this person/section?	0	1							
		(Confirm	Cancel					

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

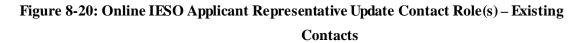
Alternatively, the Applicant Representative can choose the 'By Role' selection to retrieve all applicable roles for their organization's active participations. This will result in a list similar to the one shown in Figure 8-19.

A	elect Contac				
0	rganization ID: 122846				
	Organization: ENERCO Request Type: Update C				
	allable Cor ct Rol				
	A. I.	a(a)			
	All of the o each conta contact rol	contact role(s) fisted below are contact role(s) that can be assigned based on your organization's existing sct role. The minimum and maximum number of contacts permitted and the current number of contacts at is you want to update and select next.	participation(s) your organizati	The table provid on in each role. F	les a descriptio Nase select (†
	Contact Role Name	Description	Min. Required	No. of Existing	Max. Permitte
	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	
	Authorized Representative	Person responsible for contractually binding your organization with the IESO. This role assigns Primary Contacts.	1	0	8
	Bids and Offers	Person or Section responsible for submitting and/or changing real-time bids or offers for your organization.	D	1	
	Compliance and Market Surveillance	Person responsible for discussing participant conduct and activities within the IESO- administered markets for your organization.	D	0	
	Day-Ahead-Bids and Offers	Person or Section responsible for submitting and/or changing day-shead bids or offers for your organization.	D	0	*
	Dispatch Data Submitter	Person or Section responsible for submitting and/or changing real-time bids or offers for your organization.	1	2	*
	Dispetch Data Viewer	Person or Section responsible for viewing and/or changing real-time bids or offers for your organization.	1	0	-
	Emergency Preparedness Plan	Person responsible for submitting and updating the Emergency Preparedness Plan for your organization.	1	1	×
	Equipment Outage Late Notification Contact	Person responsible for receiving email notification on outages that are late to start and taking appropriate actions.	0	1	-
	Equipment Outage Submitter	Person responsible for submitting, updating and canceling outage request on equipment owned or operated by your organization.	1	2	3
	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.	D	1	
	Equipment Registration Specialist	Person responsible for registering equipment/resource for your organization.	1	10	3
	Information Technology	Person or Section responsible for communicating with the IESO about information technology services, projects and changes for your organization.	0	1	2
	Invoicing and Banking	Person responsible for submitting and maintaining, or approving banking information for your organization.	1	1	4
	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 submittale and data requests. In case of potential non-compliance, submitting Self-Reports and providing associated mitigation plans.	D	0	
	Market Participant Escalation Contact	Person responsible for reporting reliability compliance on escalated matters (due dates are missed) under the Ortanic Reliability Compliance Program for your organization. This person is preferably of higher authority than the person designated as the Market Participant Compliance Contact.	D	0	×
	MMP Meter Trouble Report	Person responsible for monitoring Meter Trouble Reports, adding comments, and receiving Meter Trouble Reports status notifications.	1	1	
	Notice of Disagreement	Person responsible for submitting Notices of Disagreement for settlement statements for your organization.	1	1	4
	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	4
	Revenue Metering	Person responsible for viewing the master data for registered meter installations and in-fight data submitted during a meter registration request. The Revenue Metering Contact for a transmitter organization is responsible for approving Sile Registration Reports for transmission delivery points.	1	1	
	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	
	Settlements	Person responsible for issues/questions relating to settlement statements for your organization.	0	D	
ж	1-22 of 22 🛞 🛞	415 (1980-1997) 1			
		d Help? News less nairegistration help#1.22			

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.

News	Tasks	Records	s Re	eports	Actions			Alex Apprep -	Appian
🥵 i	ieso	QA		date (Contact Rol	le			
		Cont	ganization D: 12346 Organization: ENERCON Executive Uddate Contact Role(s) by Role tact Role Details Charges 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 a perior, sector or both. Contact Role Details Contact Role Details III Contact Role Details III 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 perior, sector or both. Maximum 1 Perepaired: Contact Type; Perior						
				ting Con					
						or section(s) are currently assigned to the Disputor both 'Dispatch Data Submitter' role and 'Disp			
				Contact		Person ID	Person/Section	Status	
				Person		510359	John Koetsier	Existing	
				Person		516080	Peter Primary	Existing	
					Need Help? http://www.leso.c	alregistration, helpi¥1,23	Done Cancel	Remove Person Add Pe	erson



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.

News Tasks Records	s Reports	Actions		Alex Apprep - Appiar						
😵 ieso 🛚	Update Contact Role Request Details									
	Organization ID: Organization: Request Type: Contact Role I	ENERCON Update Contact Role(s) by Role								
	Contact Role Name: Minimum Required: Maximum Permitted: Contact Type: Existing Conta	- Person								
		The following person(s) or section(s) are currently assigned to th Contact cannot have both 'Dispatch Data Submitter' role an								
	Contact	Person ID	Person/Section	Status						
	Person	507488	Bob Smith							
	Person	510359	John Koetsier	Existing						
	Person	516080	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.

ws Tasks Records	Reports	Actions			Alex Apprep -	Appian			
🖗 ieso 🛚	Update Contact Role Request Details								
	Organization ID: Organization: Request Type:								
	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 Depatch Dats Submitter Name: Minimum Contacts Required: Contact Type: Person Contact(s) to be Added								
	Contact		Person ID	Person/Section					
	Person		507486	Bob Smith					
	Contact(s) Su	mmary							
		This is the list of cont	act(s) that will be assigned to the contact role after	you click 'Confirm'.					
	Contact		Person ID	Person/Section					
	Person		507488	Bob Smith					
	Person		510359	John Koetsier		_			
	Person		516080	Peter Primary					
					Confirm	cel			

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.

News	Tasks (4)	Records	Reports	Actions	🔝 Richard RightsAdmin -	# -	Appian
(Sei 🚱	so			Organizatior cation you are representing) while completing this action.		
		Orga	anizations				
			Name				
			ACME GENE	RATION			
			NEW ECO GE	ENERATION			
			BIGSTEAM G	SENERATION			
			HIGH TENSI	ON NETWORKS			
			MUSKOKA	NETWORKS			
			PROVINCIAL	LDISTRIBUTION			
			CITIES DISTR	RIBUTION			
			TRIPLE A NE	TWORKS			
			GITCHIGUN	I DISTRIBUTION			
			🔹 1-9 of 9 🕟	. 8			
		* Requ	uired		Next	Ca	incel

Figure 8-25: Choose an Organization Page

News	Tasks	Records	Reports	Actions	📘 Richard Rightsadmin - 📲 -	<i>A</i> ppian
🤗 ies	0	:	Select Sys	tem Acc	ess Request Type	
			Request Details			
			Organization:	ACME GENER	RATION	
			System Access	Request Type	•	
			Select:	Grant Access Grant Access Revoke Access	Role(s)	
					Next	ancel
		,	* Required			

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.

News	Tasks (4)	Records R	eports	Actions	🔝 Richard RightsAdmin -	🛿 - Appian
Pies	so	Select	Acco	ount Type		
		Request	Details			
		Organiz	tation ID	999999		
		Orga	nization	ACME GENERATION		
			Access est Type	Grant Access Role(s)		
		Assignee	е Туре			
				access role(s) can be assig communications. Machine a	ned to a personal account meant for use by a registered personed to a machine account to accommodate Application Progra counts have a custodian, the registered person responsible f ccount type for this access role assignment.	am Interface (API)
			• Select	Person		
		* Required			Next	Cancel

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.

News	Tasks (4)	Records Report:	s Actions	🔝 Richard RightsAdmin -	🐮 - Appiar						
eiesc)	Search for	r a Registered P	erson							
		Request Details									
		Organization II	999999								
		Organization	ACME GENERATION								
		System Access Request Type	s Grant Access Role(s) e								
		Account Type	e Person								
		Search for a Re	Search for a Registered Person								
	Person II Last Nam First Nam	accurate results. At least one the person can then be registe	on using the following search fields. Enter complete inform field must be filled in for the search. If the person is not fou red.								
		*Required		Seach for Person	Cancel						

Search and Select a Registered Person

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 grant ticket issued to the IESO, the instructions to create an account for the person with an automatically assigned User Name. Once IESO ITOPS Customer Support creates the actual account, the Registration system will email the person with the user account name details

News	Tasks (4)	Records	Reports	Actions	1	Richard Right	sAdmin -	:: - Appian	
eso		Sel	ect Regi	stered Pers	on				
		Req	uest Details						
		Or	ganization ID	999999					
			Organization	ACME GENERATION Grant Access Role(s)					
			stem Access Request Type						
		,	Account Type	Person					
		Search Results							
			Person ID	Last Name	First Name	Preferred Name	Middle	Name	
			Person ID	Last Name	First Name	Preferred Name	Middle	Name	
			507433	Somer	Em				
		×	Person ID Last Name First Name	K K somer em	ieve the person you w	ere searching, by again by r	modifying the sea	rch fields below.	
		*Req	uired		Next	efine Search Registe	r New Person	Cancel	

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) 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
- b) 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

	Tasks (4)	Records	Reports	Actions	🚨 Richard R	ightsAdmin -	tt - Appia		
eies	0	Regi	ster a l	New Person					
		Reque	st Details						
		Orga	nization ID	999999					
		Or	ganization	ACME GENERATION					
			em Access quest Type	Grant Access Role(s)					
		Acc	count Type	Person					
					mation below. The address fields i s but can be modified. Please note				
		Person	Person Information						
			First Name		* Address Line 1				
		•	Last Name		Address Line 2				
		* M	lain Phone		Address Line 3				
				Example: 123-456-7890	Address Line 4				
			Lain Phone Extension		* City				
				Numbers only	Province/State	N/A	•		
		.,	Main Email			Outside Canada or US	SA, select N/A		
					* Postal Code/Zip				
					Code	Example: R3T 2T5 or unknown, use N/A	12345. lf		
					* Country	Canada			
							Next		
		*Require	ed.						

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.

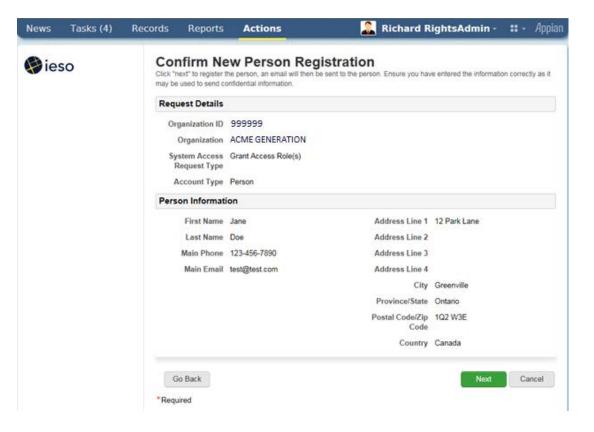


Figure 8-31: Confirm New Person Registration Page - Grant

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 Grant or Revoke requests from being submitted to the IESO 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*.

F

5	Tasks (4)	Records	Reports	Actions	🤶 Richard RightsAdmin - 📰 - Ap						
es	0	Sel	ect Acce	ss Role(s)	to be Granted						
		Request Details									
		Or	ganization ID	999999							
			Organization /	ACME GENERATIC	N Contraction of the second seco						
			System Access Grant Access Role(s) Request Type								
		,	Account Type								
			Person	lane Doe							
		Person ID 507435									
		Exis	Existing Access Role(s)								
		Role	Name		Description						
					No items available						
			🔹 1-1 of 0 🕞	н							
		Aco	Access Roles								
		Finan	cial Market Oper Role Name	ations/Settlements							
			Financial Mark Trading & Rep	et Submit Tr orts applicatio	ansmission Rights Auction bids via the Transmission Rights Auction n. Retrieve financial market reports via the IESO Participant Reports site.						
			Financial Mark Reports	arket Retrieve financial market reports via the IESO Participant Reports site.							
		🗑 🛞 1-2 of 2 🔅 🖻									
		Partic	ipation Settleme	ints							
			Role Name	D	scription						
		12	Settlements Settlements Re	uutinssiuti o E	ubmit & search settlement information via the Online Settlement Request rm system. Retrieve settlement reports via the IESO Participant Reports e.						
	8	Settlements Settlements Re	earch & Se eports sy	arch settlement information via the Online Settlement Request Form stem. Retrieve settlement reports via the IESO Participant Reports site.							
		Notice Of Disa Submission		ubmit notices of disagreement via the Workflow Notice of Disagreement stem.							
	13	Settlements Reports		trieve settlement reports via the IESO Participant Reports site.							
		1-4 of 4 🕑 H									

Select Access Roles to be Granted



The Rights Administrator should in the case of granting access roles to the person, choose <u>only</u> 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

News	Tasks (4)	Records	Reports	Actions	🙎 Richard RightsAdmin -	# -	Appian		
() ie:	so			st that will be granted to this	to be Granted person or machine account with this request.				
		Request Details							
		Or	rganization ID	999999					
			Organization Name	ACME GENERATION					
			ystem Access Request Type	Grant Access Role(s)					
		1	Account Type						
			Person	Jane Doe					
			Person ID	507435					
		Acc	Access Role(s) to be Granted						
		Access Roles to Confirm for Account							
		Role	Name	Description					
		Final Trad	Rights Auction bids via the Transmission Rights Auction ket reports via the IESO Participant Reports site.	applicat	tion.				
			Financial Market Reports Reports via the IESO Participant Reports site.						
		8	N 🕢 1-2 of 2 🕑 H						
		0	Go Back		Confirm	Ca	incel		
		*Req	uired						

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 a grant ticket to IESO ITOPS Customer support to enroll the person's account in the access roles requested.

News	Tasks (4)	Records Reports	Action	🔒 🔝 Richard RightsAdmin - 📰 - Appia					
Pies	50	Select Acc	ess Role	(s) to be Revoked					
		Request Details	Request Details						
		Organization ID	999999						
		Organization	ACME GENER	ATION					
		System Access Request Type		Role(s)					
		Account Type							
		Person	Jane Doe						
		Person ID	507435						
		Existing Access Roles							
		Revenue Metering-	access roles to						
		Role Name	8	escription					
		Revenue M MVWeb & N	MP Pernets	few tabular displays of revenue metering data and download metering text files is the MVWEB system. Retrieve MMP reports via the IESO Participant Reports te.					
		🛞 🛞 1-1 of 1	8 🛞 1-1 of 1 🛞 8						
				Next Revoke All Cancel					
		*Required							

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 <u>only</u> 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

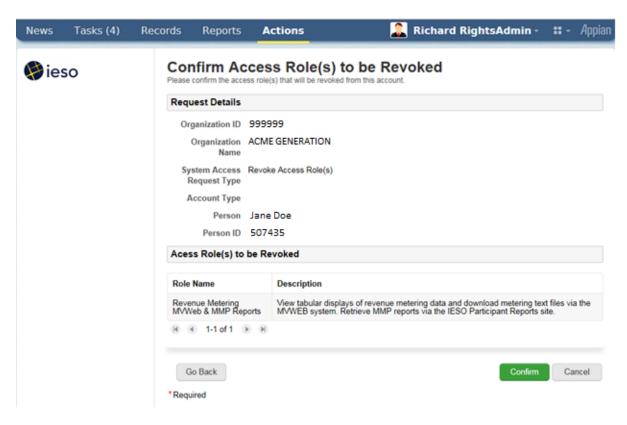


Figure 8-35: Confirm Access Role(s) to be Revoked Page

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 a revoke ticket to IESO ITOPS Customer support to remove the association that the person's 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.

News	Tasks (4)	Records Repor	ts Actions	🚨 Richard RightsAdmin -	• 🐮 • Appian
Pies	so	Select Ma	chine Account		
		Request Detai	ls		
		Organization	ID 999999		
		Organizati Nar	ACME GENERATION		
		System Acce Request Ty	ss Grant Access Role(s)		
		Account Ty	pe Machine		
		Search for Ma	chine Account		
		Machine Accou	ID below. If you need a new m	ole(s) to an existing machine account, please provide the aachine account, select 'New Machine Account'. the account ID	machine account
		*Required		Next New Machine Account	nt Cancel

Figure 8-36: Select Machine Account Page - Grant

News	Tasks (4)	Records Report	s Actions	🚉 Richard RightsAdmin - 💷 - Appian				
eso		Select Ma	chine Account					
		Request Detail	5					
		Organization I	D 999999					
		Organizatio Nam						
		System Acces Request Typ	s Revoke Access Role(s) e					
		Account Typ	e Machine					
		Search for Machine Account						
		Machine Accour I Warnin	nt Please use the exact case of g If your organization requir that you already have and	trount ID of the machine account for which access role(s) are to be revoked. If the account ID es continued use of access role(s) that you are about to revoke, ensure ther machine account with the required access role(s). By revoking needed, your organization may not be capable of conducting business				
		Go Back * Required		Next Cancel				

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.

News	Tasks (4)	Records Reports	Actions	🧟 Richard RightsAdmin - 💷 - Appi	an			
eso		Confirm E	xisting Machine	e Account				
		Request Details						
		Organization II	999999					
		Organization Name						
		System Access Request Type	Grant Access Role(s)					
		Account Type	Machine					
		Machine Account Details						
				ided has the following custodian. Select 'Next' if this is the right custodian to ccount. If the custodian listed below is not right, select 'Go Back' to search				
		Machine Account						
		Person ID	507370					
		First Name	F. Allen					
		Last Name	Wiley					
		Go Back		Next Cancel	ľ			

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 *IESO* ITOPS Customer Support will 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.

News	Tasks (4)	Records	Reports	Actions	🚨 Richard RightsAdmin -	🐮 – 🛛 Appia	an
() ies	60			hine Accou	nt for Access Role Grant		
		Reque	st Details				
		Orga	nization ID	109120			
		Or	rganization I Name	BJ ENERGY LLC			
			em Access quest Type	Grant Access Role(s)			
		Acc	count Type	Machine			
		New M	lachine Acc	ount Information			
				Please provide the IP (I) account.	nternet Protocol) address for the API to be associated with this new	machine	
		Go	Back		Next	Cancel	
		*Require	ed				

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

Once the Rights Administrator has either:

- a) Confirmed an existing machine account to be used or
- b) 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.

Tasks (4)	Records Reports	Actions	🚨 Richard RightsAdmin - 🗰 - Appi				
eso	Select Access Role(s) to be Granted						
	Request Details	(
	Organization ID	999999					
	Organization	ACME GENERA	TION				
	System Access Request Type	Grant Access Rol	e(s)				
	Account Type	Machine					
	Person (Custodian)	F. Allen Wiley					
	Person ID	507370					
	Machine Account Id						
	Existing Access	s Role(s)					
	Role Name		Description				
	No items available						
	H 4 1-1of0 IN H						
	Access Roles						
	Financial Market O	needed based on t	(s) to assign. The access role(s) listed correspond to the access role(s) that may be re organization's participation.				
	Role Name		Description				
	Financial M	larket Reports API	Retrieve financial market reports via the IESO Participant Reports site.				
	(H 3) 1-1 of 1 (E H)						
	Participation Settle	ments					
	Role Name		Descilption				
	Settlements Reports API Retrieve settlement reports via the IESO Participant Reports ste.						
	(8 8) 1-1 of 1 (8 16)						
	* Required		Next Carvel				

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 <u>only</u> 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.

News	Tasks (4)	Records	Reports	Actions	🚨 Richard RightsAdmin - 🟥 - Appian				
() ieso			Confirm Access Role(s) to be Granted Please confirm the access that will be granted to this person or machine account with this request.						
		Req	uest Details						
		Or	rganization ID	999999					
			Organization Name	ACME GENERA	TION				
			ystem Access Request Type	Grant Access Ro	le(s)				
		1	Account Type	Machine					
			Person (Custodian)						
			Person ID	507370					
		Mac	hine Account ID	APIIESO00014					
		Acc	Access Role(s) to be Granted						
		Acces	s Roles to Cor	firm for Account					
		Role	Name		Description				
		Fina	ncial Market Re	ports API F	Retrieve financial market reports via the IESO Participant Reports site.				
		Settl	Settlements Reports API		Retrieve settlement reports via the IESO Participant Reports site.				
		i € 1-2 of 2 → H							
			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 a grant ticket to *IESO* ITOPS Customer support to enroll the 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 a revoke ticket to *IESO* ITOPS Customer support to remove the association that the machine account has with the access roles requested.

8.1.4 Registration System Mange 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.

News	Tasks	Records	Reports	Actions	Richard Right	sadmin -	🐮 - Appian
		C	Choose an	Action For Richard F	Rightsadmin		
		1	Action to comple	ete			
			Action	Update Person Information			•
		*	Required			Continue	Cancel

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.

IS	Tasks	Records	Reports /	Actions		Richard Rightsadmin →		, ibbiai
			Update Per Please make any upda	rson Information For tes to your person information below.	or Richard Rightsadmin			
			Person Informat	ion				
			Person ID	507437	* Main Email	test@test.ca		
			Position		Alternate Email 1			
			* First Name	Richard	Alternate Email 2			
			* Last 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		* Postal Code/Zip	M5V 3Y3		
					Code * Country	Canada		•
					Contact Notes	oundu		
					condernotes			
							Conti	nue
			*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.

News	Tasks	Records	Reports 🖌	Actions		📕 Richard Rightsadmin -	:: -	<i>A</i> ppian
					ation For Richard Rightsadmi y as it may be used to send confidential information.	n		
			Person Informati	on				
			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			
				123-123-5678	Address Line 4			
			Alternate Phone 1		,	Toronto		
			Alternate Phone 2		Province/State			
			Fax Number		Post Code/Zip Code	M5V 3Y3		
					Country	Canada		
					Contact Notes			
								_
						Finish Back	Can	cel
			*Required					

Figure 8-43 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 change person ticket in the background to *IESO* ITOPS Customer Support to request an update to any associated accounts for the person record with those attribute values. This will ensure that any user personal and machine account information is kept up to date 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* Portal, Online IESO system, Reports site, Energy Market Interface (EMI), Prudential system and Outage Management (OM) system etc. can be changed or reset via 3 separate methods.

- Password change on first time login to the Portal or after verbal request to the *participant* Rights Administrator or IESO Customer Relations to have their password reset and a new temporary password issued to the user. Once the password has been changed on login to the Portal, the account may be used with the Portal, Online IESO system, Report site, Energy Market Interface or Outage Management system etc.
- Password Self Recovery during Portal, Energy Market Interface or Outage Management system login when a user as Forgotten their Password. This can only be done logging into those systems but not the Online IESO system or IESO Reports site. The user must have already selected their five security questions and answers to do this self-recovery.
- Password normal manual change after login via the Portal's 'Security Profile' password change capability located on the 'Security Profile' page

Note: The Portal, Online IESO, IESO Reports Site, Energy Market Interface and Outage Management System all use common single User Accounts. Changes to the password for a User Account within the Portal for example will automatically be applicable and usable for login to the Online IESO system, Reports site, Energy Market Interface and Outage Management System.

The user can and should after logging in to the Portal for the first time, select a personal security image and phrase along with five security questions 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.).

- The user selected security image and phrase will be presented to the user during each subsequent login to the Portal. If they do not see the chosen image and phrase the user should suspect the authenticity of the Portal login pages. The security image and passphrase can be changed afterwards via the Security Profile page in the Portal.
- Five questions can be selected from a randomly produced short list from a larger number of possible predefined choices. The choices made available should meet all users' possible circumstances. Each user will be presented with different combinations of choices.
- Once the five security questions have been selected and answers input, the question choices can be changed after Portal logon at any time via the Security Profile page in the Portal.
- The answers to the security questions are not 'case sensitive' and can use any ASCII characters. However, the user should select 5 security questions that permit 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 Temporary Password Change

1) If the user is logging in for the first time to the Portal, EMI or OM system or if the *IESO* Customer Relations has had the user's password reset (based on request or a security need) then the user will be prompted to change the password when the attempt to login is made. Once the user has input their valid User Account (shown in Figure 9-1) and clicked on the "Continue" button he/she will be prompted to enter their password (shown in Figure 9-2). Note that the user should typically use lower case for their user account name on first time and subsequent logins and to set their security questions. The security system distinguishes between upper and lower case so a user account entered as upper case after first using lower case (or vice versa) will be seen as different and trigger a request for new security questions.

	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
Sign In with User Account Name and Password	Links:
Enter your User Account Name.	Where do Lenter my password?
User Account Name: Continue Attention to Market Participants accessing the Transmission Rights Auction and Energy Market, Outage Management and Settlement Forms applications: This portal is owned and operated by the ESO, and all use of this portal is governed by the ESO's market rules. As a registered Market Participant, you have received a unique and confidential User Account and Password from the IESO to access this portal and you agree to maintain their confidentially by sharing them with only your authorized representative(s). You specifically agree that you are exclusively responsible for all access to and any activity on this portal that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized access or use of your User Account and Password. If you do not agree with these terms and conditions, do not login to this portal and immediately advise the IESO.	 Log In Tips Forgot User ID? Forgot User ID/Password? Not a registered user? For Assistance: Contact IESO Customer Relations Tel: 905-403-6900 Toll-Free: 1-888-448-7777 Fax: 905-403-6921 E-mail: customer.relations@ieso.ca

Figure 9-1: Portal / Identity Management Login – User Account Name Entry

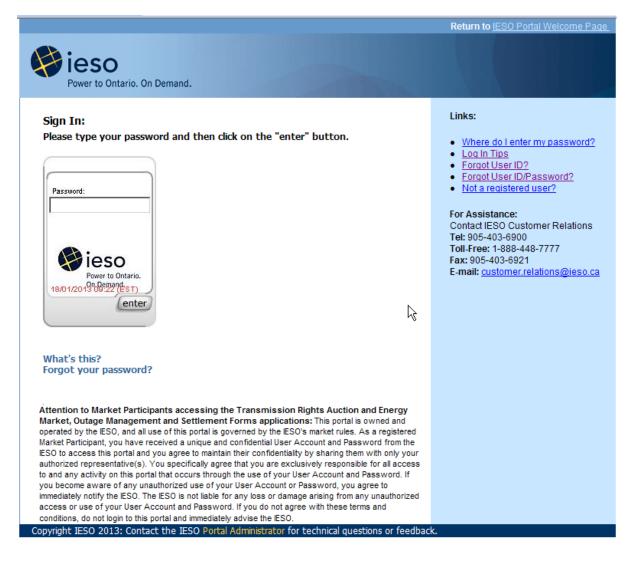


Figure 9-2: Portal / Identity Management Login – Password Entry

- 2) After entering the password and clicking on the 'Enter' button the user will be presented with a change password page where they will be able to enter in the old password and then the new password twice as shown in Figure 9-3.
- 3) If the password entered was incorrect of if the user entered the wrong user account name for the password the user will see an error message as shown in figure 9-4 and the user may try again.

		Return to IESO Portal Welcome Page
Vert to Ontario. On Deman	d.	
password and click "enter", th Choose a new password that • Case sensitive (The "Cap • Eight characters or long • Contains all of the follo • upper-case • lower-case • special character	en type it again and click " is easy to remember and me os Lock" key should be off) jer wing three types: [NOTE - Do not use the follo ss than sign), > (greater th	ou will then be able to create a new password. Type new enter" to confirm your password and continue your log-in. eets these password rules: owing special characters in your password: & (ampersand), \ fan sign), ' (single quote), " (double quote).]
Old Password	click to type	
New Password Confirm New Password	click to type	Password:
Copyright IESO 2013: Contact the I		Power to Ontario. 18/01/2019 Begggtest enter

Figure 9-3: Portal / Identity Management Login – Password Reset

	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
Sign In with User Account Name and Password Enter your User Account Name. Sorry, the identification you entered was not recognized. Please try again.	Links:
User Account Name:	Forgot User ID/Password? Not a registered user? For Assistance:
Attention to Market Participants accessing the Transmission Rights Auction and Energy	Contact IESO Customer Relations Tel: 905-403-6900 Toll-Free: 1-888-448-7777 Fax: 905-403-6921
Market, Outage Management and Settlement Forms applications: This portal is owned and operated by the IESO, and all use of this portal is governed by the IESO's market rules. As a registered Market Participant, you have received a unique and confidential User Account and Password from the IESO to access this portal and you agree to maintain their confidentiality by sharing them with only your authorized representative(s). You specifically agree that you are exclusively responsible for all access to and any activity on this portal that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized	E-mail: <u>customer.relations@ieso.ca</u>
access or use of your User Account and Password. If you do not agree with these terms and conditions, do not login to this portal and immediately advise the IESO. Copyright IESO 2013: Contact the IESO Portal Administrator for technical query ons or feedbac	k.

Figure 9-4: Portal / Identity Management Login – User Account Name and/or Password Error Message

4) Once the 'Reset Your Password' page is presented the user must enter in their temporary password (Old Password) again and then their new password and its confirmation as shown in Figure 9-5 and then click on the "Enter" button. The new password must meet the displayed rules and must not have been used in recent history before. If the account is brand new this will not be an issue.

		Return to IESO Portal Welcome Page
Vertex Contario. On Dema	nd.	
password and click "enter", t Choose a new password that • Case sensitive (The "Ca • Eight characters or Ion • Contains all of the folk • upper-case • lower-case • special character	hen type it again and click ' : is easy to remember and m ps Lock" key should be off ger owing three types: r [NOTE - Do not use the fol ess than sign), > (greater t	•
Old Password	Completed	
New Password	Completed	Password:
Confirm New Password	click to type	
Copyright IESO 2013: Contact the		Power to Ontario. Power to Ontario. 18/01/2019 UP 30 PERSON enter

Figure 9-5: Portal / Identity Management Login – Password Reset

- 5) If the temporary password entered is incorrect, or if the new password entered does not meet the required rules or has been used recently before. If the two new password entries do not match, then an error message will be displayed as shown in Figure 9-6 and the user can try again.
- 6) However, if the user first enters the current old password incorrectly, she/he will not be shown an error message until the 'old password', 'new password' and 'confirm new password' has been entered and the 'Enter' button has been clicked. The error message as shown in Figure 9-7 will display and the user can start over.

		Return to IESO Portal Welcome Page
Power to Ontario. On	Demand.	
password and click "end Choose a new passwor • Case sensitive (T • Eight characters • Contains all of th • upper-case • lower-case • special che (backslash • Includes no spac	issword below and click "enter". You wi ter", then type it again and click "enter d that is easy to remember and meets t he "Caps Lock" key should be off) or longer he following three types: e aracter [NOTE - Do not use the following), < (less than sign), > (greater than si	II then be able to create a new password. Type new " to confirm your password and continue your log-in. chese password rules: g special characters in your password: & (ampersand), \ gn), ' (single quote), " (double quote).]
Old Password	Completed	
New Password	New passwords entered do not match.	Password:
Confirm New Password	New passwords entered do not match.	Power to Ontario. 18/0 1/20 19 US 1990 (EST) enter
Copyright IESO 2013: Conta	ct the IESO Portal Administrator for technica	I questions or feedback.

Figure 9-6: Portal Identity Management Login Page – Change Password - Mismatch Error

		Retu	rn to IESO Portal Welcome Page
Power to Ontario. On Dema	nd.		
password and click "enter", t Choose a new password that Choose a new password that Eight characters or lon Contains all of the folk Oupper-case Iower-case Special character (backslash), < (I Includes no spaces Please make sure the "	hen type it again and click "e : is easy to remember and me aps Lock" key should be off) ger owing three types: r [NOTE - Do not use the folk ess than sign), > (greater th	wing special characters in your pa an sign), ' (single quote), " (doubl	nd continue your log-in. assword: & (ampersand), \
Old Password	click to type		
New Password	click to type	Password:	\searrow
Confirm New Password	click to type	×	
		Power to Ontario. 18/01/2013 NORMATEST) enter	
pyright IESO 2013: Contact the	IESO Portal Administrator for teo	hnical questions or feedback.	

Figure 9-7: Portal Identity Management Login Page – Change Password - Old Password Error

- 7) Once the user has typed in the valid temporary password and entered in a valid new password and its confirmation, when the "Enter" button is clicked on the password will be changed and the user will be informed of a successful password change by an email notification immediately as shown in Figure 9-8. Note that this email message is also normally sent when an IESO administrator resets the user account password when requested to do so by the authorized user or the register MPRO.
- 8) If all conditions on the user's workstation are OK, the user should be logged in and then be prompted to set up the new user account 'Security Profile' as shown in Figure 9-9. The user is permitted to skip setting up the security profile once. If they choose to do so, on the next login to the Portal the Security Profile setup is mandatory and the user will be automatically redirected to the pages to do that. If during login there is any issue on the workstation such as another Portal session in the IE browser active etc. the user will likely see a technical error message as shown in Figure 9-10. This can be ignored as a nuisance issue. The user can re-enter the account name and new password and login will proceed. The email notification is the proof that the password has been successfully changed.

Dear IESO User,

Your IESO Account password has been reset. This was done either because:

- 1. You changed your password in your IESO Portal Security Profile or
- 2. You requested a password reset from the IESO or
- 3. You were prompted to change your password during login.

If your password was reset by the IESO upon your request, you will receive a new one-time password shortly.

If you did not change your password or request a password change from the IESO, please contact IESO Customer Relations at (905-403-6900, Toll-Free 1-888-448-7777) immediately.

Thank you,

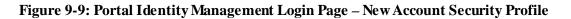
Ι

IESO Identity Management Services

***** This is a system generated mail please do not reply. *****

Figure 9-8: Portal Identity Management – Change Password Notification Email

	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
 Set Up Your New Account Security Profile Setting up your new account security profile is required to enhance your of security to your account by helping you identify our site and helping us id This involves two steps: Select a personal image and phrase. Choose five security questions and answers that only you will know you to remember, but very difficult for others to discover or guess, answers in the future, neither you nor the IESO will be able to record not know or ever ask you for your questions and answers. These features will be used to enhance your account security when loggin you to change your own password online. If you choose to skip this step today, you will be required to complete it refor assistance, please click on the help file or contact IESO Customer Related to the provident of the prov	entify you. Be sure to enter answers that will be easy for While you can change your questions and ver the answers you enter now. IESO staff will g in to the IESO Portal. They will also allow next time you log on.
A personal image and phrase is now in use for enhanced security. This personalized authentication device will help you safeguard your IESO account from potential compromise. Presentation of the image and phrase combination that you choose, along with a date and time stamp that is less than 24 hours old, provide proof that you are connecting to the official IESO Portal. If the image and phrase presented during sign on do not match your selection you should stop and contact IESO Customer Relations immediately. Never share your account information with other people.	This is an example of a personalized TextPad
Security questions and answers are now in use to add an additional layer of security. You need to register five security questions. When visiting the IESO Portal, you may be asked to answer one or more of these questions (please ensure that your personal image and phrase are correct before doing so). When choosing your questions and entering your answers be sure to select those that will be easy for you to remember, but very difficult for others to discover or guess. While you can change your questions and answers in the future, neither you nor the IESO will be able to recover the answers you enter. IESO staff will not know or ever ask you for your questions and answers. These should be kept secret like a password.	Ouestions (choose a spectrum time month balance) Answers 1. [rinder year weak your signal ward after board? If 2. [rinder weak your signal ward after board? If 3. [rinder weak your signal ward after board? If 4. [rinder weak your signal ward after board? If
If you decide not to complete	registration at this time click >> Skip
	account security profile now >> Continue
Copyright IESO 2013: Contact the IESO Portal Administrator for technical questions or	feedback.



	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
Sign In with User Account Name and Password Enter your User Account Name. A technical error has occurred. Please try again.	Links:
User Account Name:	Forgot User ID? Forgot User ID/Password? Not a registered user?
Continue Attention to Market Participants accessing the Transmission Rights Auction and Energy Market, Outage Management and Settlement Forms applications: This portal is owned and operated by the IESO, and all use of this portal is governed by the IESO's market rules. As a registered Market Participant, you have received a unique and confidential User Account and Password from the IESO to access this portal and you agree to maintain their confidentiality by sharing them with only your authorized representative(s). You specifically agree that you are exclusively responsible for all access to and any activity on this portal that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized access or use of your User Account and Password. If you do not agree with these terms and conditions, do not login to this portal and immediately advise the IESO. pyright IESO 2013: Contact the IESO Portal Administrator for technical questions or feedbace	For Assistance: Contact IESO Customer Relations Tel: 905-403-6900 Toll-Free: 1-888-448-7777 Fax: 905-403-6921 E-mail: customer.relations@ieso.ca

Figure 9-10: Portal Identity Management Login Page – Login Technical Error

- 9) If the user experiences too many unsuccessful attempts (i.e. 5) at logging in with an incorrect temporary password the user's account will be automatically locked out. If this happens the login page will just keep indicating that the users account credentials are not recognized as shown in Figure 9-4 above. Under such conditions the user can choose to wait until the account is unlocked automatically by the system (1 hour) and attempt again to change the temporary password or contact IESO Customer Relations for assistance. The same is true for an enduring password but with such the user can attempt password self-recovery with the security questions if they have already defined their security questions. If they have not defined their security questions, password self-recovery cannot be done by the user.
- 10) When the user chooses to register their Security Profile by clicking on the 'Continue' button for such as shown in Figure 9-9 then he/she will be prompted to set up the new user account 'Security Profile' image and phrase as shown in Figure 9-11. The user can click on the Get a new image and phrase as many times as desired until he/she sees a suitable combination. The chosen image and phrase will be 'presented' during subsequent logins to the Portal so that the user has confidence she/he is connecting to the valid IESO Portal. If the user does not see the chosen image /phrase combination, the authenticity of the website is suspect and the user should stop and call the IESO.



Figure 9-11: Security Profile – Choosing a Security Image and Phrase

11) Once the user is happy with the image and phrase combination the 'Continue' button should be clicked on to save the choice and continue to the selection of security questions and input of answers. The user can then choose each of the 5 question choices and input answers as shown in Figure 9-12. The user should choose questions that he/she can easily remember the answers for consistently without effort. Note that the user's chosen image and phrase is shown on the Security Questions page to validate that the user has not been redirected to some other website.

		A REAL PROPERTY AND ADDRESS OF	Return to IESO Portal Welcome
F	ieso		
	Power to Ontario. On Demand.		
	reverse oncario, on permana.	ALC: NO DE CONTRACTOR DE C	A CONTRACTOR OF A CONTRACT
fou com	curity Questions ir chosen security questions and answers will be used uplete this step, click on a question from the random It will be easy for you to remember but very difficult f	y generated drop-down list. C	noose questions with answ
ase	t will be easy for you to remember but very difficult f e sensitive) after you are sure you are seeing your per stion.	sonal image and phrase. Click	enter" to choose the next
-			
n I	Questions (Choose a question from each set of choir Select One	ces below)	Answers
.,	Dalaw Olla		ER AL
2)	Select One	×	Prove and
			and the second second
3)	Select One	*	Arswer L. R.
1		1000	Sup transmission
			wet stakes
0	Select One	×.	and summer
	Select One		eturn to IESO Portal Welcome
			etum to IEBO Portal Welcome
			etum to (ESO Portal Welcome
Sec You con tha cas	pht IESO 2013: Contact the IESO Portal Administrator for te	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	firm your account identity.
Sec	pht IESO 2013: Contact the IESO Portal Administrator for to IESO Power to Ontario. On Demand. curity Questions ar chosen security questions and answers will be used notes the say for you to remember but very difficult for te sensitive) after you are sure you are seeing your per estion.	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity oose questions with answe Type the answer (they are enter' to choose the next
Sec	pht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ar chosen security questions and answers will be used molete this step, click on a question from the randomy t will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choic	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity oose questions with answe Type the answer (they are enter' to choose the next
Sec You con tha cas que	ht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. Curity Questions ar chosen security questions and answers will be used mplete this step, click on a question from the randomy t will be easy for you to remember but yery difficult for te sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choix What was your father's profession when you were born?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity oose questions with answe Type the answer (they are enter' to choose the next
Sec	pht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ar chosen security questions and answers will be used molete this step, click on a question from the randomy t will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choic	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity oose questions with answe Type the answer (they are enter' to choose the next
Sec You con thas que 1)	ht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. Curity Questions ar chosen security questions and answers will be used mplete this step, click on a question from the randomy t will be easy for you to remember but yery difficult for te sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choix What was your father's profession when you were born?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity oose questions with answe Type the answer (they are enter' to choose the next
Sec You con thas que 1)	yht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ur chosen security questions and answers will be used polete this step, click on a question from the randomh it will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choix What was your favourite cartoon character as a child?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity, oose questions with answer Type the answer (they are enter" to choose the next Answers
Sec You con thas que 1)	ht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ar chosen security questions and answers will be used molete this step, clack on a question from the randomy t will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choid What was your father's profession when you were born? What was your favourite cartoon character as a child? What was the first street you lived on?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity, oose questions with answe Type the answer (they are enter" to choose the next Answers
Sec You con thas que 1) 2) 3)	yht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ur chosen security questions and answers will be used polete this step, click on a question from the randomh it will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choix What was your favourite cartoon character as a child?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity, oose questions with answe Type the answer (they are enter" to choose the next Answers
See You case que 1) 2) 3) 4)	ht IESO 2013: Contact the IESO Portal Administrator for to Power to Ontario. On Demand. curity Questions ar chosen security questions and answers will be used molete this step, clack on a question from the randomy t will be easy for you to remember but very difficult for e sensitive) after you are sure you are seeing your per estion. Questions (Choose a question from each set of choid What was your father's profession when you were born? What was your favourite cartoon character as a child? What was the first street you lived on?	whenever it is necessary to cor y generated drop-down list. Ch or others to guess or discover, sonal image and phrase. Cick "	nfirm your account identity, oose questions with answe Type the answer (they are enter" to choose the next Answers

Figure 9-12: Security Profile – Choosing Security Questions and Inputting Answers

9.1.2 Password Self Recovery

- If the user has forgotten the password but has entered and knows the answers for their security questions chosen for their account, they will be able to create and enter a new password via the Identity Management login pages by selecting the "Forgot your Password?" Link as shown in Figure 9-13 after they have entered the User Name
- 2) Clicking on the "Forgot your Password?" link will navigate the user to the first page providing the capability to allow the user to reset their password, as displayed in Figure 9-14. The user will be presented with 2 or 3 of their 5 security questions in sequence, to which the correct answers must be provided, in order to be able to reset the password. The chosen image and phase will be

shown at all times on the pages to validate the authenticity of the web pages. If the user remembers the password in the middle of the procedure and stops the password reset and then restarts the browser and then logs in with the remembered password, the system based on the security policy may ask a security question after the correct password has been entered to confirm identity.

	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
Sign In: Please type your password and then click on the "enter" button.	Links: • Where do Lenter my password? • Log In Tips • Forgot User ID? • Forgot User ID? • Not a registered user? For Assistance: Contact IESO Customer Relations Tel: 905-403-6900 Toll-Free: 1-888-448-7777 Fax: 905-403-6921 E-mail: customer relations@ieso.ca
What's this? Your chosen image and personal phrase in the TextPad is not shown? Fordot your password?	
Attention to Market Participants accessing the Transmission Rights Auction and Energy Market, Outage Management and Settlement Forms applications: This portal is owned and operated by the IESO, and all use of this portal is governed by the IESO's market rules. As a registered Market Participant, you have received a unique and confidential User Account and Password from the IESO to access this portal and you agree to maintain their confidentiality by sharing them with only your authorized representative(s). You specifically agree that you are exclusively responsible for all access to and any activity on this portal that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree to immediately notify the IESO. The IESO is not liable for any loss or damage arising from any unauthorized access or use of your User Account and Password. If you do not agree with these terms and conditions, do not login to this portal and immediately advise the IESO.	

Figure 9-13: Portal Identity Management Login Page - Forgot Password Option

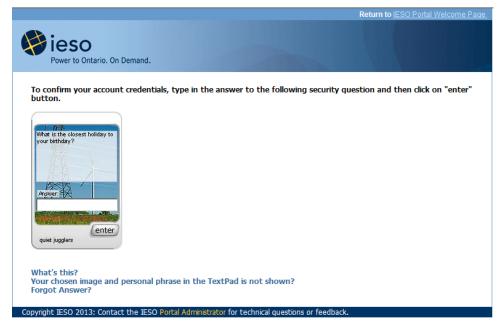


Figure 9-14: User Account Password Reset - Security Question Challenge Example

3) An invalid answer to a security question will result in an error message as shown in Figure 9-15. The correct answer to each question must be input in order to proceed and input a new password. Entry of an incorrect answer repeatedly 5 times will lock the user's security profile and account. If this happens a page will display indicating that the user is not authorized to login and to contact customer service as shown in Figure 9-16. The user should contact IESO Customer Relations and if he/she is able to provide sufficient confirming information regarding their identity, will be provided a new one-time password. The IESO will also reset the security profile back to null so the user, once they login with the new temporary password will have to set up their security profile image, phrase and 5 security questions again as described above.

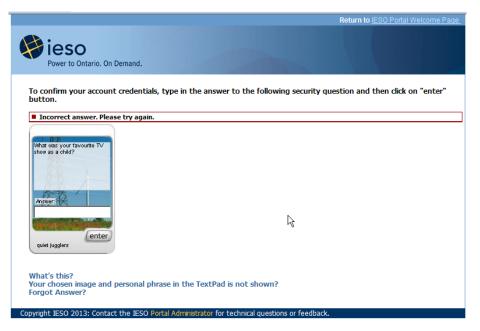


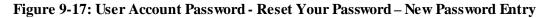
Figure 9-15: User Account Password Reset – Invalid Answer Provided

	Return to IESO Portal Welcome Page
Power to Ontario. On Demand.	
Sign In with User Account Name and Password Enter your User Account Name.	Links: Where do Lenter my password? Log in Tips
You are not authorized to login. Please contact customer service. User Account Name:	Forgot User ID? Forgot User ID/Password? Not a registered user?
Continue	For Assistance: Contact IESO Customer Relations Tel: 905-403-6900 Toll-Free: 1-888-448-7777
Attention to Market Participants accessing the Transmission Rights Auction and Energy Market, Outage Management and Settlement Forms applications: This portal is owned and operated by the ESO, and all use of this portal is governed by the ESO's market rules. As a registered Market Participant, you have received a unique and confidential User Account and Password from the ESO to access this portal and you agree to maintain their confidentially by sharing them with only your authorized representative(s). You specifically agree that you are exclusively responsible for all access to and any activity on this portal that occurs through the use of your User Account and Password. If you become aware of any unauthorized use of your User Account or Password, you agree immediately notify the ESO. The ESO is not lable for any loss or damage arising from any unauthorized	Fax: 905-403-6921 E-mail: <u>customer relations@leso.ca</u>
accessory use of your User Account and Password. If you do not agree with these terms and conditions, do not login to this portal and immediately advise the IESO. Copyright IESO 2013: Contact the IESO Portal Administrator for technical questions or feedbac	k.

Figure 9-16 User Account Password Reset – Account Locked

4) Once entries of the correct answers to the security question have been input and the "Enter" button is clicked, the next page allowing the user to input their new password will be displayed. This is shown in Figure 9-17. The user must enter in a new password that has not been used very recently before. Note that the system will remember quite a few passwords used previously.

		Return to IESO Portal Welcome Page
Power to Ontario. On Den	nand.	
Choose a new password th Case sensitive (The " Eight characters or la Contains all of the fo oupper-case olower-case ospecial charact	at is easy to remember and mo Caps Lock" key should be off) onger sollowing three types: ter [NOTE - Do not use the folk (less than sign), > (greater th	then type it again and click "enter" to confirm your password. eets these password rules: owing special characters in your password: & (ampersand), \ an sign), ' (single quote), " (double quote).]
New Password	click to type	
Confirm New Password	click to type	Password: Password:
Copyright IESO 2013: Contact th	e IESO Portal Administrator for te	chnical questions or feedback.



5) If the user enters in a password already used in the recent past and is still known by the system password history, or if the password entered does not meet the rules as displayed clicking on the "Next" button will display an error message indicating that a problem was encountered. This is shown in Figure 9-18. The user must enter in a new password that meets all policy conditions.

 Case sensitive (The "Caps Lock" key should be off) Eight characters or longer Contains all of the following three types: upper-case lower-case special character [NOTE - Do not use the following special characters in your password: & (ampersand), (backslash), < (less than sign), > (greater than sign), ' (single quote), " (double quote).] Includes no spaces Please make sure the "Num Lock" key is off 			Return to IESO Portal Welcome Pag
 Construction function of the second point of the second p		nd.	
ose a new password that is easy to remember and meets these password rules: Case sensitive (The "Caps Lock" key should be off) Eight characters or longer Contains all of the following three types: oupper-case obwer-case special character [NOTE - Do not use the following special characters in your password: & (ampersand), (backslash), < (less than sign), > (greater than sign), ' (single quote), " (double quote).] Includes no spaces Please make sure the "Num Lock" key is off four new password does not meet the password policy requirements. Please try again. Password click to type firm New Password click to type cli	Reset Your Password		
 Eight characters or longer Contains all of the following three types: upper-case lower-case special character [NOTE - Do not use the following special characters in your password: & (ampersand), (backslash), < (less than sign), > (greater than sign), ' (single quote), " (double quote).] Includes no spaces Please make sure the "Num Lock" key is off Yeassword does not meet the password policy requirements. Please try again. <i>Please make sure the click to type</i> firm New Password click to type <i>Click to type Click to t</i>			
r Password click to type firm New Password click to type	 upper-case lower-case special characte (backslash), < (I Includes no spaces Please make sure the ' 	r [NOTE - Do not use the fo less than sign), > (greater t 'Num Lock" key is off	than sign), ' (single quote), " (double quote).]
firm New Password click to type	•		quirements. Please try again.
rejoicing athletes	New Password Confirm New Password		
ht IESO 2013: Contact the IESO Portal Administrator for technical guestions or feedback.			

Figure 9-18: User Account Password Reset Step 3 of 4 – Invalid New Password Entry

- 6) Once a user has entered in a new password that meets all password policy rules and clicked on the next button on the password, the password will be accepted and reset and the user logged into the Portal. The user will also receive an email notification of the password change as shown in Figure 9-8. However, the user may be asked other security questions afterwards as well as dictated by the security policies
- 7) Upon entering a new password and logging in, if the user sees a screen similar to the one shown in Figure 9-19 (Sandbox Portal example) then the newly created user account created by the IESO has not been automatically activated within the Portal as it should have been. The user should contact IESO Customer Relations to inform them of the problem so that the account can be activated.

🖉 Log In - Windows Internet Explorer	
COO - Ittps://portalsandbox.ieso.ca/portal/server.pt?cache	d=false&space=Login 🔽 🔒 🄄 🗙 😫 Google
File Edit View Favorites Tools Help	
🚖 Favorites 🛛 🚖 🙋 SB OAM 🙋 QA Portal 🙋 QA Oracle Acc	ess Manager 📲 RBC Login 🖉 Prod OAM 🥖 Prod Portal
🔡 🕶 🌈 Log In 🛛 🗙 😣 Google	🚵 🔻 🖾 🝸 🖶 🖶 Vage 🗸 Safety 🗸 Tools 🗸
My Home Welcome, Guest Log In	Help 31-Jan-2013 9:52:50 AM
My Communities 🔻	
(*) Ieso	Log In
Power to Ontario. On Demand.	
Welcome to your	r portal.
Log in to your perso	onalized portal account.
	ting account, enter your user name and password. the appropriate authentication source. If you want
to log in to the port and then click Log I	al automatically, select Remember my password , (n.
User name:	
Password:	
Authentication source:	DMZ-SBX Authentication So V
	Remember my password
	Log In
Copyright IESO 2012: For technical ques	tions or feedback about the IESO portal, contact the Portal Administrator

Figure 9-19: User Account Login – Welcome to your Portal Login Page Displayed

9.1.3 Navigating to the User Security Profile Page

In order to normally change the User Account security image/phrase, password or change the security questions and answers defined on initial login, the user must navigate to their security profile page. This can be done after login by clicking on the "Check your Portal Security Profile" page tab as shown in Figure 9-20. This is a Sandbox Portal example; the Production environment is similar.

My Home Welcome, Jones John B. My	Account Log Off
My Communities IESO Sandbox	Neb P
Connecting Today. Powering Tomorrow.	IESO Sandbox Web Portal Welcome IESO Home
🖄 Inside This Community 🔻	
IESO Home Check your Portal Security Pro	ile and a second se
IESO Related Web Links	IESO Web Portal
IESO Public Website	Welcome to the IESO Web Portal. This site will be the future home for most market-related applications and information. The applications currently available through this site
	are:
Portal User Guide	Settlements
IESO Reports Site	
	The Settlements community pages allow you to retrieve meter data and submit settlement data on-line.
IESO Sandbox Reports Site	
	Transmission Rights Auction (TRA)
IESO Outage Submission Tool	The TRA community pages provide access to the auction application, related communications, reports and information - all from one location.
Dispatch Service Sandbox System	the net commany pages prome access to an access appreciation, reacce commandations, reports and mornated in an non-net or focusion.
IESO Contact Info	Energy Market Application
S Error	The Market Tradino portal community is the new home for the sandbox Energy Market application (i.e. MPI Worksnace) formerly accessed via MOSWEBH using a digital

Figure 9-20: Typical Portal Home Page with Security Profile Tab

- 1) This will activate the security profile page which will display the IESO Security Profile portlet shown in Figure 9-21 which is linked to the Identity Management system's security profile page. The user can, via the security profile page:
 - a) Get a new security image and phrase 'Get a new image and phrase'
 - b) Reset the security questions and answers 'Reset your questions and answers'
 - c) Change the user account password 'Change your password'

IESO Home Check your Portal Security Profile IESO Security Profile Personal image and phrase preferences This is your personal image and phrase combination. To change it, click on "Get a new image and phrase". You may repeat this until you have an image and phrase you like. To keep this new image and phrase, simply leave the page. You may also click on links below to reset your questions and answers or to change your password.	e Check your Portal Security Profile
Personal image and phrase preferences This is your personal image and phrase combination. To change it, click on "Get a new image and phrase". You may repeat this until you have an image and phrase you like. To keep this new image and phrase, simply leave the page. You may also click on links below to reset your questions and answers or to change your password.	
This is your personal image and phrase combination. To change it, click on "Get a new image and phrase". You may repeat this until you have an image and phrase you like. To keep this new image and phrase, simply leave the page. You may also click on links below to reset your questions and answers or to change your password.	scurity Profile
 Your personal security image Your personal security phrase Learn more Get a new image and phrase Reset your questions and answers Change your password 	Personal image and phrase preferences This is your personal image and phrase combination. To change it, click on "Get a new image and phrase". You may repeat this new image and phrase, simply leave the page. You may also click on links below to reset your questions and answers or to change your password. Image and phrase preferences Image and phrase preferences You may also click on links below to reset your questions and answers or to change your password. Image and phrase preferences Image and phrase Image and phrase

Figure 9-21: Portal Security Profile Page - Personal Image and Phrase Preferences

- 2) 'Get a new image and phrase' will refresh the page shown in Figure 9-21 with a new image and phrase. The user can continue to click on the 'Get a new image and phrase' link to update the combination until one that is suitable is presented.
- 3) 'Reset your questions and answers' will refresh the page shown in Figure 9-22 with one for selecting new Security Questions and entering new answers. The user must select five questions from the presented dropdown selection list and enter the answer for each. If the user stops selecting new questions and entering answers before the fifth and final one the selections will not be saved. Only when the fifth question and answer is entered are all five of the questions and answers saved.
- 4) 'Change your password' will refresh the page shown in Figure 9-23 with the fields shown for entering the old and new passwords. The user must complete all fields and click on the "Enter" button for each before the new password is committed to the system.

🟠 Inside This Community 🔻				
IESO Home Security Profile				
IESO Securit	Security Profile			
	You com that case	curity Questions or chosen security questions and answers will be used whenever plete this step, click on a question from the randomly generate t will be easy for you to remember but very difficult for others a sensitive) after you are sure you are seeing your personal imagestion.	ed drop-down list. (to guess or discove ge and phrase. Click	Choose questions with answers r. Type the answer (they are not "enter" to choose the next
		Questions (Choose a question from each set of choices below)		Answers
	1)	Select One Select One If you needed a new first name, what would it be?	- To	
	2)	What is the most unusual job you have had? What is the name of a university you applied to but did not attend? How much did you pay for your first car? What is your spouse's nickname?		
	3)	Select One	~	Answer:
	4)	Select One	~	encouraging gorillas
	5)	Select One	~	

Figure 9-22: Portal Security Profile Page – Security Questions

🖄 Inside Th	nis Community 🔻			
IESO Home	Security Profile			
IESO Secu	rity Profile			
	 Case sensitive (The "C. Eight characters or lor Contains all of the foll upper-case lower-case special character 	aps Lock" key should be off iger owing three types: r [NOTE - Do not use the fo less than sign), > (greater t	r and meets these password rules: ;) illowing special characters in your password: & (ampersand), \ than sign), ' (single quote), " (double quote).]	
	Old Password	click to type		
	New Password	click to type	Password:	
	Confirm New Password	click to type	encouraging gonllas	

Figure 9-23: Portal Security Profile Page – Change Your Password

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

10.2 Java 2 Runtime Environment for the Portal with Internet Explorer 11

There is no longer any need for a Java 2 Runtime Environment on a client workstation for use with the Portal with Internet Explorer 11 or any other browser.

A number of years ago Oracle took possession of Java with its acquisition of Sun Micro Systems. Almost immediately the java security model was impacted. All java applets became governed by the content of the java security policy files on the users' workstations. At first this was not an issue as the java policy file needed was located in each user's home directory on the C drive of the workstation. It was relatively easy for the IESO to create a standard java security policy file and publish it and have the end users of the MPI application and Portal, both of which used java applets for uploading files to the respective servers, download and install the file in their own home user directory.

More recently Oracle changed their java security model such that only the java policy file located in the java (JRE) install location on the users' workstations is recognized. Multiple file upload functionality within the Portal collaboration communities ceased to work. The IESO was able to resurrect the functionality by determining what the content of the java install security policy file needed to be and have MPs and internal users download and instruct their respective IT departments to update the file. This however was administratively intensive as market participant IT support personnel had to look after maintaining the java policy file on end user workstations.

However, with the latest versions of JRE updates the Portal multiple file upload applet ceased to function again. The IESO decided to look for an upgrade for multiple file functionality and found a solution.

A JavaScript based multiple file upload functionality was found by a product called "FineUploader". A consultant to other companies using the same portal software found a way to use this product to upgrade the portal software to enable multiple file upload functionality without the need for a java runtime environment on client workstations. The solution can be leveraged by any application for multiple file uploading and this is what the IESO did for the Portal collaboration application. Within the collaboration application a few files were updated and the needed "FineUploader" files were added. The updated collaboration application was used to replace the existing one on the Portal server where it resides.

To the end user there is only a superficial look and feel change in how multiple file upload functionality works in the Portal. The same popup window is activated, navigation and searching for files to upload works exactly the same as before but drag and drop of files onto the upload window functionality is now available. Files are added to a list in the window in the order chosen not alphabetically. Clicking on the Upload button triggers the upload to proceed the same as before. Thermometer bar progress of files being uploaded is displayed and success file uploads are highlighted in green when complete. Upload failure of any file is highlighted in magenta. Typically any attempt to upload files with the listed metacharacters (/ : *? " <> | #.",") will result in a generic error such as: "Error on file number # - filename: Reason upload failure reason unknown". Correcting the name of the file will allow it to be uploaded. There is a hard coded 1 GB file size limit

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:

- Internet Explorer browser to access the Energy Market Interface (EMI) web server. 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 <u>address</u> using your Internet Explorer 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)

ß	
This signed IESO MIM Web Services provides the programmatic API to submit/download MIM data using SOAP based web services. This version of the API requires two part of authentication: UserID/Password and whitelisted client machine IP address. <u>Quick Reference Guide</u>	
Last Updated	Aug 11, 2016
Document	zip WSDL XSD

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.

Ref.	Task Name	Task Detail
A.01	Obtain Internal Approval and communicate 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 a Rights Administrator within the <i>participant</i> , the IESO system access requirements (Sandbox and/or Production environment). The Credential Subscriber should communicate to the Rights Administrator what access permissions they are internally approved for.
A.02	Submit request for User Account and Contact role and/or System access permissions via Online IESO Registration System	The Rights Administrator (or applicant representative) logs in to the Sandbox and/or Production Online IESO Registration system(s) and performs 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.

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

Ref.	Task Name	Task Detail
A.03	Receive Grant/ Revoke access ticket task from online Registration system. Validate grant/revoke information. Create User Account and assign to requested access roles.	ITOPS Customer Support receives a Grant/ Revoke access ticket task from online Registration system. They will validate the request to ensure the account does not already exist (i.e. conflict with another person's personal or machine account). They will then create a user account for the Credential Subscriber and enroll the account in the requested access roles. ITOPS does not need to enroll the account in any contact roles as this is completed in IESO Online. When the ticket has been closed the system will issue an email to the Credential Subscriber with the User Account Name to be used.
A.04	Provide User Account Name's temporary Password to Credential Subscriber.	ITOPS Customer Support will provide the User Account Name's temporary Password to Credential Subscriber via a phone call to the registered main phone number for the person.
A.05	Receive User Account Name and temporary Password. Reset password on first login where applicable	The Credential Subscriber will receive the User Account Name's temporary Password via a phone call from ITOPS Customer Support and proceed to the initialization process to update to login to the IESO Portal, update the temporary password to one of their own choosing and set the account's security questions as per section 9 in 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.

Ref.	Task Name	Task Detail
B.01	Obtain Internal Approval and communicate 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 a Rights Administrator within the <i>participant</i> the IESO system access requirements (Sandbox and/or Production environment). The Credential Subscriber should communicate to the Rights Administrator the existing user account information, Person ID and

 Table A-2: Account Change Scenario 1 Task Details

Ref.	Task Name	Task Detail
		what access permissions are internally approved for granting or revoking.
B.02	Submit request for change to a user account's access / Contact roles / system access permissions via online Registration System	The Rights Administrator (or applicant representative) submits a grant or revoke request for changes to a user account's access / Contact roles / system access permissions (personal or machine account) via IESO Online Registration System as per Section 8 of this document. Participation contact role changes made take effect immediately.
B.03	Receive Grant/ Revoke access ticket task from IESO Online Registration system. Validate grant/revoke information.	ITOPS Customer Support receives a Grant/ Revoke access ticket task from the IESO Online Registration system. They will validate the request to ensure the account does exist and its current 'access role' permissions.
B.04	Arrange for updating Credential Subscriber of system access permissions for requested user account to access roles assignment. Notify Subscriber	ITOPS Customer Support will arrange for updating Credential Subscriber system access permissions for the requested user account to 'access roles' assignment within the IESO. When complete they will notify the Subscriber where applicable.
B.05	Receive confirmation of changes.	The Credential Subscriber will receive confirmation of the access role changes from the IESO where applicable and feasible.

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.

Ref.	Task Name	Task Detail
C.01	Update the person record in the IESO Online Registration System where applicable and then 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 system. This will automatically generate a change person ticket to IESO ITOPS Customer Support to make the required changes to the associated user account(s) for the person.
C.02	Receive Person change ticket task from IESO Online Registration system. Validate user account attribute change information.	IESO ITOPS Customer Support will receive the Person change ticket task from IESO Online Registration system. They will validate the user account attribute change to make sure it is complete and does not conflict with any existing active account(s).
C.03	Arrange for modified credentials (Name, User Account Name, email address, phone no.) Notify Subscriber of implemented changes.	IESO ITOPS Customer Support will make or arrange for the modifications credentials (person name, User Account Name, email address, phone no.) and notify the Subscriber of the implemented changes where required.
C.04	Receive change notification	The Credential Subscriber receives the account change information notification from ITOPS Customer Support where feasible and applicable.

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

A.4 Participant User Account Deactivation Scenario

A *participant* Rights Administrator requests a User Account 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 Deactivation Scenario.

Ref.	Task Name	Task Detail
D.01	Communicate removal of systems access permissions and desired account deactivation with Rights Administrator	A Credential Subscriber (or Primary Contact in cases where person has left <i>participant</i>) communicates the need for removal of the person's systems access permissions and desired account deactivation with Rights Administrator.
D.02	Remove selected person's access/ Contact role(s) for selected organization and where applicable request account deactivation via IESO Online Registration System	The Rights Administrator (or applicant representative) submits a revoke access role(s) request for all of the selected person's access 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	Receive Grant/ Revoke change ticket task from IESO Online Registration system. Validate grant/revoke information.	<i>IESO</i> ITOPS Customer Support receives a Grant/ Revoke change ticket task from IESO Online Registration system and validates that the grant/revoke information is for an existing account(s)
D.04	Arrange for disabling of systems access privileges and deactivation of User Account where applicable.	<i>IESO</i> ITOPS Customer Support will arrange for disabling of the targeted person's User Account(s) systems access roles / privileges and deactivation of the User Account(s) where applicable. <i>IESO</i> ITOPS 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.

Table A-4: Participant User Account Deactivation Scenario Task Details

Ref.	Task Name	Task Detail
	Notify Rights Administrator of disabling of systems access for User Account(s) and deactivation of user account(s) where no longer required.	
D.05	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.

Ref.	Task Name	Task Detail
E.01	Use provisioning tools if existing to recover credentials or replace forgotten identity credentials password using user defined security questions and answers. Else communicate need to recover account password with <i>IESO</i> Customer Relations	An Individual Subscriber or Application Subscriber attempts to self- recover their User Account password where possible with the <i>IESO</i> provided on-line provisioning tools where existing or can call <i>IESO</i> Customer Relations for support where self-recovery functionality is not available for some accounts or where self-recovery is unsuccessful. In the case where password self-recovery works the process ends.
E.02	Receive and validate request to recover account password.	<i>IESO</i> Customer Relations will receive and validate the request to recover an account password.
E.03	Arrange for recovery of User Account password, Where applicable, provide new temporary password to Credential Subscriber and/or arrange for unlocking of account where required or	<i>IESO</i> Customer Relations will either reset the Credential Subscriber's password where possible or arrange for recovery of User Account password, and where applicable, provide a new temporary password to Credential Subscriber and/or arrange for unlocking of account where required or provide the replacement password to the subscriber.

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

Ref.	Task Name	Task Detail
	provide replacement password to subscriber.	
E.04	Receive new temporary password for User Account or replacement password for applications that do not support one time password.	The Credential Subscriber will receive new temporary password for User Account or replacement password for applications that do not support one time password from <i>IESO</i> Customer Relations or <i>IESO</i> ITOPS Customer Support.

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.

Ref.	Task Name	Task Detail
F.01	Use online provisioning tools if existing to recover credentials or replace forgotten identity credentials password using user defined security questions and answers. Else communicate need to recover account password with IESO Customer Relations.	A Rights Administrator will use the online provisioning tools if existing to recover credentials or replace forgotten identity credentials password using user defined security questions and answers. If this fails, the Rights Administrator can communicate the need to recover their account password with <i>IESO</i> Customer Relations. In the case where password self-recovery works the process ends.
F.02	Receive and validate request to recover Rights Administrator account password.	<i>IESO</i> Customer Relations will receive and validate the request to recover Rights Administrator account password.
F.03	Arrange for recovery of User Account password, Provide new temporary password to Rights Administrator and/or arrange for unlocking of account where required.	<i>IESO</i> Customer Relations will either reset the Rights Administrator's password where possible or will arrange for recovery of User Account password and provide a new temporary password to Rights Administrator and/or arrange for unlocking of account where required.
F.04	Receive new temporary password for User Account or replacement password for	The Rights Administrator will receive new temporary password for User Account or replacement password for applications that do not support one-time password from <i>IESO</i> Customer Relations or <i>IESO</i> ITOPS Customer Support.

 Table A-6: Account Recovery Scenario 2 Task Details

26.0 – November 3, 2020

Ref.	Task Name	Task Detail
	applications that do not support one time password.	

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.

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.	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. 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 a grant/revoke request to <i>IESO</i> ITOPS Customer Support to create the account.
G.02	Receive Grant/ Revoke access ticket task from Online IESO Registration system. Validate grant/revoke information. Create User Account and assign to Online IESO Registration System access role for external users.	 <i>IESO</i> ITOPS Customer Support will receive a Grant/ Revoke access ticket task from online Registration system. They will validate grant/revoke information to ensure there is no conflict with existing user accounts. <i>IESO</i> ITOPS Customer Support will then create the User Account and assign it to the Online IESO Registration System access role for external users. When <i>IESO</i> ITOPS Customer Support sets the User Account name, the Online IESO Registration System will email the Rights Administrator with the User Account Name.
G.03	Forward User Account Name / temporary password. Confirm User	<i>IESO</i> ITOPS Customer Support will forward the User Account Name's temporary password to the Rights Administrator and confirm the User Account name and password with the Rights Administrator.

 Table A-7: Rights Administrator Enrolment Scenario Task Details

26.0 – November 3, 2020

Ref.	Task Name	Task Detail
	Account name and password with Rights Administrator	
G.04	Receive User Account Name and temporary password from IESO ITOPS Customer Support	The Rights Administrator will receive the User Account Name via email and the temporary password from <i>IESO</i> ITOPS Customer Support by phone call. He or she can then proceed to initialization of the account by navigating in a browser to the <i>IESO</i> Portal and logging in with the account (Sandbox and/or Production) See scenario A-12

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.

Ref.	Task Name	Task Detail
H.01	Update own person record in the Online IESO Registration system where applicable and in the process communicates the need to update their User Account information to <i>IESO</i> ITOPS Customer Support.	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 communicates the need to update their User Account information to <i>IESO</i> ITOPS Customer Support by automatically issuing a grant/revoke person change ticket.
H.02	Receive Grant/ Revoke person change ticket task from Online IESO Registration system. Validate Rights Administrator change information.	<i>IESO</i> ITOPS Customer Support will receive a Grant/ Revoke person change ticket task from the Online IESO Registration system. They will validate Rights Administrator user account attribute change information to make sure it is complete and does not conflict with any existing active account(s).
H.03	Arrange for modified credentials (Name, User Account Name,	<i>IESO</i> ITOPS Customer Support arranges for modified credentials (Name, User Account Name, email address, phone no.) and then notify the Rights Administrator of implemented changes where possible.

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

Ref.	Task Name	Task Detail
	email address, phone no.)	
	Notify Rights Administrator of implemented changes.	
H.04	Receive change notification of credential updates.	The <i>participant</i> Rights Administrator will receive a change notification of his or her credential updates from <i>IESO</i> ITOPS Customer Support 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.

Ref.	Task Name	Task Detail
I.01	Obtain Internal Participant approval for system access permission change.	The Rights Administrator obtains internal <i>participant</i> approval for system access permission change (Sandbox and/or Production).
I.02	Submit request for change to own or other Rights Administrator's (for same Participant) user account's access /Contact roles / system access permissions via Online IESO Registration System	A Rights Administrator submits a request for change to his or her 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). The Registration System (Sandbox and/or Production) will automatically send a Grant/Revoke ticket to <i>IESO</i> ITOPS Customer Support with the requested changes. Participation contact role changes made, take effect immediately via the IESO Online Registration System.
I.03	Receive Grant/ Revoke access ticket task from Online IESO Registration system. Validate Grant/Revoke information.	<i>IESO</i> ITOPS Customer Support will receive a Grant/ Revoke access ticket task from the Online IESO Registration system (Sandbox or Production). They will then validate the Grant/Revoke information for the access roles to be granted or revoked.
I.04	Arrange for update to Rights Administrator's user account to access roles assignment /	<i>IESO</i> ITOPS Customer Support will arrange for updating the Rights Administrator's user account to access roles assignment / system access permission. They will then notify the Rights Administrator where possible of the implemented access role changes.

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

Ref.	Task Name	Task Detail
	system access permissions. Notify Rights Administrator	
I.05	Receive confirmation of changes.	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.

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.

Ref.	Task Name	Task Detail	
J.01	Remove selected person's Rights Administrator role assignment for selected organization and where applicable	A Primary Contact removes the selected person's Rights Administrator 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. If the person still need an <i>IESO</i> user account, the process is complete.	
	request account deactivation via Online IESO Registration System where applicable.	If the Primary Contact submits access role changes and/or the person no longer needs an <i>IESO</i> account the Registration System (Sandbox and/or Production) will automatically send a Grant/Revoke ticket to <i>IESO</i> ITOPS Customer Support with the requested changes.	
J.02	Receive Grant/ Revoke change ticket task from Online IESO Registration system. Validate grant/revoke information.	<i>IESO</i> ITOPS Customer Support will receive a Grant/ Revoke change ticket task from Online IESO Registration system (Sandbox or Production). They will then validate the Grant/Revoke information for the access roles to be revoked.	
J.03	Arrange for removal of the person's User Account's Registration System access and other access privileges and	<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	

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

Ref.	Task Name	Task Detail
	deactivation of the account where applicable. Notify Primary Contact of deactivation of user account and removal of system access privileges where possible	
AA.04	Receive notification of de-activation of Rights Administrator's credential and removal of system access privileges.	The Primary Contact will receive notification of de-activation of Rights Administrator's credential (Sandbox or Production) and removal of system access privileges where possible.

A.11 Subscriber User Account Initialization

Initialization of a Participant Contact's User Account.

Once the *participant* representative is registered for a User Account through the Online IESO Registration System, he/she will receive a User Account / Password.

The User Account password, (one time or enduring as applicable) once delivered to the Credential Subscriber can be used immediately.

For more information on system functionality relating to the tasks described below, refer to sections 9 and 10 of this guide.

Ref.	Task Name	Task Detail	
K.01	Access the web based Identity Management provisioning tools through the <i>IESO</i> Portal login for initializing a User Account for the Portal.	If not already done; upon receipt of User Account / password (one time or enduring) for initial issuance or recovery: For a User Account / Password identity credential used with the Portal, Online IESO System, Report site, Energy Market Interface or Outage Management System (Sandbox or Production where applicable); the <i>participant</i> person shall access the <i>IESO</i> Portal login (Sandbox or Production) for initializing/using a User Account and resetting the temporary password with one of the user's choosing.	
K.02	Use the tool to activate the required identity credentials.	Use the Portal login (Sandbox or Production) to enter in User Account and temporary password.	
K.03	Validate User Account / Temporary Password, input new password.	For user Account / Password Identity Credentials used with the Portal, the <i>IESO</i> Identity Management System will validate the User Account and one time password and request the user change their password to one of the user's choosing	
K.04	Use web based identity management provisioning tool to re-enter correct identity credential activation codes /information	The Credential Subscriber uses the Portal's identity management provisioning tool functions to re-enter the correct User Account and temporary password. If the User Account and temporary password do not work for any reason the initialization process will have to be terminated and the user will have to request appropriate help from the <i>IESO</i> Customer Relations/ Identity Management Officer.	
		Note: If the person's User Account / temporary password is known to be correct but does not work then it is possible that the data was	

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

Ref.	Task Name	Task Detail
		intercepted and used to initialize a security profile illegally or more likely there is a technical issue with the <i>IESO</i> systems. While the chance of User Account password interception is remote, if the user suspects this has occurred, the user must inform <i>IESO</i> Customer Relations so that the problem can be verified with the Identity Management system where appropriate. The User Account's temporary password will be reset and resent to the User. In the case where a user's account is locked it will be unlocked.
K.05	Receive User Account / activation confirmation. Choose security image and phrase, security questions and input answers.	The User Account's successful password change / reset is confirmed within the Portal login web pages to the end user. The person will then need to choose a Portal login security image and phrase, and select their security questions and input answers. When complete the person will be able to use the User Account to login to the Portal, Online IESO System, Energy Market Interface, Report site or Outage Management System where granted access / Contact roles permit.

A.12 Periodic Update of Subscriber User Account Password

Ref.	Task Name	Task Detail
L.01	Login to the IESO Portal with a User Account	For the Portal a User Account and password (Sandbox or Production) can be used to login. Security questions selected by the user in the OAAM component may also be posed to which the correct answer must be provided.
L.02	Check for password renewal and initiate password change process if required.	The Portal OAM and OAAM Identity Management components shall check to see if password update is required and notify the user.
L.03	No notification of update received at Portal Identity Management tools. Use Portal etc. as required for normal business operations.	If no notification of imminent User Account password expiry is received at the Portal OAM and OAAM Identity Management tools then the user can use it as required to access the <i>IESO</i> Portal, Registration System, Report site or Reliability Compliance Tool normal business operations.
L.04	Portal Identity Management tools sends User Account password prompt user to change password.	The Portal OAM and OAAM Identity Management tools send the user a prompt to change their password.
L.05	Change password in Portal Identity Management using old password or security questions to enable change.	The user shall follow the instructions on the Portal Identity Management web pages to change their password to a new one that meets the password rules.

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).

Access Role(s) change – The 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 process.

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 Primary Contact are aware of inaccuracies, a Registration system request should be submitted by the 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).

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 process.

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 or Primary Contact is aware of inaccuracies, a Registration system request should be submitted by the 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 Mark et 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 ITOPS Customer Support - is responsible for receiving user Account and system access role /permission request and for performing account creation and issuance, name changes, access role changes and user Account deactivation.

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.

Mark et 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.

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

Capacity Mark et 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 Mark et Participant-MMP - The organization is responsible for the financial settlements with respect to a Demand Response resource.

Demand Response Mark et Participant-Operator - The organization operates a Demand Response resource.

Demand Response Mark et Participant-Owner - The organization has a Demand Response Capacity Obligation.

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

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

Distributor-Metered Mark et 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 - No definition provided

Electricity Storage Participant-MMPT - No definition provided

Electricity Storage Participant-Operator- No definition provided

Electricity Storage Participant-Owner - No definition provided

Electricity Storage Participant-RMP - No definition provided

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 Mark et Participant - The organization is responsible for the financial settlement of metering data associated with a registered generation facility.

Generator-Metered Mark et 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 Mark et 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 Mark et Participant - The organization is responsible for the financial settlement of metering data associated with a registered load facility.

Load-Metered Mark et 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 Mark et 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 Provincewide 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.

References

Document Name	Doc ID
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 -