Government of Saskatchewan

Information Circular:
Integrated Resource Information System
Security Administrator Role and Responsibilities

Document Number: RCS001

March 1, 2023

Issue Version: 1.5

Record of Change

Revision	Date	Description
0.0	June 1, 2015	Initial draft
1.0	June 22, 2015	Approved first version
1.1	August 17, 2015	Updated information on Industry Self-Declaration principle
1.2	January 22, 2020	Updated About IRIS, Terms & Definitions, Roles & Responsibilities
1.3	January 5, 2021	Updated Section 9, ER Contact information
1.4	October 1, 2021	Added Section 8 (3) Security Administrator Role Restrictions
1.5	March 1, 2023	Updated Section 3, About IRIS; Added Sections 5 (9) Security Administrator Roles and Responsibilities, and 7 (7) User Access and Management.

Table of Contents

1. INTRODUCTION

The Business Associate's (BA) Security Administrator (SA) is critical to the management and integrity of an organization's data on the Government of Saskatchewan's Integrated Resource Information System (IRIS). This *Information Circular* outlines the SA's role and responsibilities in managing IRIS accounts and permissions on behalf of a BA.

2. TERMS AND DEFINITIONS

(1) *Business Associate (BA)*

Any entity that conducts business activities with the Government of Saskatchewan through IRIS is referred to as a BA.

(2) *Business Associate Identification (BA ID)*

Every BA that conducts business with the Government of Saskatchewan through IRIS must have an active BA ID, which is a five-character numeric identification code. BAs apply to the Government of Saskatchewan for a BA ID through Petrinex (for more information on how to acquire a BA ID, go to: www.petrinex.ca).

(3) *IRIS User Accounts*

BAs have individual IRIS users within their organization, and each of those users requires an IRIS account. IRIS user accounts are set up by the BA's Security Administrator (SA). What each user can perform and see on IRIS is assigned by the SA.

(4) *Permission Sets*

Permission sets (or a group of tasks) govern what activities an IRIS user can perform in the system on behalf of the BA. To perform any activity in IRIS, the user must have the appropriate permission sets assigned to them by the BA's Security Administrator (SA). A user may have many permission sets depending on the tasks he/she is required to perform in IRIS for the BA.

(5) *Petrinex*

Petrinex is the system the oil and gas industry uses to submit volumetric, valuation, royalty taxpayer and certain infrastructure information to the Government of Saskatchewan. The Government of Saskatchewan also uses Petrinex to administer its BA ID codes. For more information about Petrinex, go to: www.petrinex.ca.

(6) *Security Administrator (SA)*

The SA is responsible for managing all of the IRIS user accounts on behalf of the BA, including assigning permissions and ensuring proper security and risk management protocols are in place to maintain the confidentiality and integrity of the BA's data on IRIS. The SA is also the default first point of contact for notifications/communications from Energy and Resources.

3. ABOUT IRIS

The Government of Saskatchewan's Integrated Resource Information System (IRIS) is an online business portal for the energy and resources industry to complete business activities and regulatory tasks with the province. For more information about IRIS, go to: https://www.saskatchewan.ca/IRIS.

4. OVERVIEW OF IRIS'S SECURITY MODEL

IRIS's comprehensive security model is designed to ensure only authorized individuals can access data or perform tasks on the system.

Security and business functions in IRIS are separated to ensure BAs can manage accountability structures within the system.

(1) *Security functions* encompass all the administrative tasks related to managing IRIS accounts and user permissions for the BA.
(2) *Business functions* are the business activities performed in IRIS on behalf of the BA (for example, applying for a full or partial waiver of Petrinex non-compliance penalties is a business function that can be performed in IRIS).

Another key component to IRIS's security is the role of the Security Administrator (SA). This individual is appointed by the Business Associate (BA) to set up, manage and administer IRIS accounts, and, importantly, assigns permissions to the BA's users that need access to both shared and confidential data in IRIS (see Section 5 for more information on the SA role).

Before a BA can gain access to IRIS, they must have:

(1) An active Business Associate identification code (BA ID). BAs are identified by a 5-character numeric ID.
(2) An appointed IRIS Security Administrator (SA).

Any person or entity that submits data to the Government of Saskatchewan on behalf of the BA will require access to the system. Potential IRIS users can span multiple areas and disciplines of an organization, and may include third-party contractors. IRIS will continually evolve and grow to include additional functionality, which in turn will expand the BA's user base.

5. SECURITY ADMINISTRATOR ROLE AND RESPONSIBILITIES

The SA has the ability to set up and assign users complete and full access to the BA's current and future data on IRIS. The SA is responsible for managing user accounts and assigning access and permissions for IRIS users within the BA or parties delegated to act on behalf of the BA.

SA responsibilities include:

(1) Create, modify and deactivate user accounts for the BA.
(2) Assign, modify and remove user permissions.
(3) Lock and unlock user accounts.

(4) Change usernames and passwords for user accounts.
(5) Set up and remove organizations delegated to act on behalf of the BA.
(6) Communicate and ensure users understand the BA's SA is responsible of managing common tasks for IRIS accounts on behalf of the BA such as password resets, unlocking or locking accounts, and creating and deactivating accounts.
(7) First point of contact for notifications/communications from Energy and Resources.
(8) Ensure users understand the terms and conditions of using IRIS, which can be found on the IRIS login page (https://iris.gov.sk.ca/Portal).
(9) If the Ministry is delegated as a SA acting on behalf of the BA, the Ministry can only manage the BA's user accounts authorized by that BA.

When the BA's application for an SA account is approved (for application information see: www.saskatchewan.ca/IRIS), the Government of Saskatchewan's Ministry of Energy & Resources, creates an SA account, and contacts the appointed SA by phone to provide an IRIS account name and password information. Once successfully logged in, the SA has access to administration screens and access to a master profile of permission sets available in IRIS. Using this master profile, the SA can begin setting up individual accounts, passwords and assigning permissions for the BA's IRIS users to complete tasks in the system.

6. ASSIGNING A SECURITY ADMINISTRATOR

As a result of the role's responsibilities, and ability to control who has full access to the BA's corporate data on IRIS, it is recommended the BA carefully consider who to assign as its SA. It is recommended the SA be an individual that:

(1) The BA trusts to control access to the organization's data on IRIS.
(2) Accepts responsibility, and fully understands the risks associated with using IRIS that could expose the BA to liability.
(3) Understands the importance of the SA role in the organization, and understands the significant work involved in managing multiple user accounts on behalf of the BA.
(4) Understands and accepts responsibility for ensuring the BA's IRIS users are fully informed of how to use the system appropriately.
(5) Ensures proper security and risk management protocols are in place to protect the BA's corporate data on IRIS.

Inappropriate use of IRIS and IRIS data by users, including the SA, is the responsibility of the BA.

7. USER ACCESS AND MANAGEMENT

It's important for the SA to understand the ramifications and risks of assigning permission sets to the BA's IRIS users. To assist the SA, here are examples to consider:

(1) The BA can acquire Crown dispositions by participating in online land sales through IRIS. If an IRIS user is provided permission to make bids on behalf of the BA, and that bid is successful, the BA is bound to honour the submission and make payment, regardless of whether the user had the authority to bid the amount tendered.

(2) In an effort to streamline and simplify government processes, IRIS operates on an Industry *Self-Declaration* principle. The BA self-declares they have met the applicable regulatory requirements upon application and/or information submission. That means, an IRIS user can declare on behalf of the BA the regulations have been met, legally binding the BA to their declaration.
(3) IRIS is a web-based application that can be accessed from any internet connection. Should an IRIS user leave the BA, or a third-party that performs work on behalf of the BA, he/she may still be able to access IRIS and the BA's data if the proper measures are not in place to deactivate the account when the BA, or the third-party employer, severs the relationship with the employee/user.
(4) An SA can delegate the security administrator responsibilities to another individual within the BA, but that individual/user will only be able to perform SA work in the system using the SA account. In addition, the BA cannot use the system to delegate the SA role to a third-party organization.
(5) Users that are delegated security administration tasks but are also required to complete business tasks in IRIS on behalf of the BA require a separate business user account in addition to having an SA account.
(6) The BA can delegate specific permissions to a third-party organization to complete business tasks in IRIS on behalf of the BA. For example:

> ABC Petroleum Company can delegate the submission of tour/drilling reports in IRIS to XYZ Drilling Company. When ABC Petroleum Company's SA assigns the permissions sets to XYZ Drilling Company, XYZ Drilling Company's SA will see the permissions in their IRIS profile. XYZ Drilling Company's SA then assigns these permissions to specific users in their organization to perform these tasks in IRIS on behalf of ABC Petroleum Company. ABC Petroleum Company's SA can set a defined time period that XYZ Drilling Company can submit drilling reports on their behalf.

It is the responsibility of the BA to ensure the necessary agreements and contracts are in place with the third-party to complete work on their behalf in IRIS. The BA is also responsible for deleting or amending permissions should the business relationship with the third-party dissolve.
(7) Mineral Rights Tax (MRT) users may choose to delegate the Ministry to act on their behalf as SA.

It is the BA's responsibility to ensure appropriate access is provided to IRIS users. The BA is responsible for all the activities performed on IRIS by its users. The following suggestions may assist in user access and management activities:

(1) Have information security and risk management practices in place, including (but not limited to):

a. Ensuring a user's level of access, and permission sets, match the user's level of authority and are the least amount of permissions required to perform their duties on IRIS.
b. Processes to manage access to IRIS should a relationship between the BA and a user be terminated.
c. For other suggestions and best practices related to information security, see:
    i. International Organization for Standardization (ISO): ISO/IEC 27001 – Information Security Management: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ii. AXELOS Global Best Practice: Information Technology Infrastructure Library (ITIL®):
https://www.axelos.com/best-practice-solutions/itil
iii. Management of Risk (M_o_R®) Best Practice Solution:
https://www.axelos.com/best-practice-solutions/mor
ITIL® - "ITIL® is a Registered Trade Mark of AXELOS Limited."
M_o_R® - "M_o_R® is a Registered Trade Mark of AXELOS Limited."

(2) Have a process to ensure the appropriate manager or supervisor approves user access to IRIS before the SA sets up an IRIS user account for the individual.
(3) Track and review access and permission sets of IRIS users periodically (e.g., every three months) to ensure users have the least amount of permissions required to perform their duties on IRIS, as well as to validate that users with an IRIS account continue to be active with the BA (or the delegated third-party) and continue to require access to IRIS.
(4) Provide training to IRIS users on the appropriate use of the system.

8. SECURITY ADMINISTRATOR ROLE RESTRICTIONS

(1) IRIS does not allow a BA to delegate the security administration permission sets to another BA or third-party.
(2) If a BA becomes inactive (i.e., as a result of an amalgamation, merger or is no longer in business, etc.), the SA account and the BA's users are deactivated by the Government of Saskatchewan to ensure users no longer have access to IRIS.
(3) The Government of Saskatchewan, at their discretion, will inactivate SA accounts and BA user accounts to ensure the integrity of the system.

9. SERVICES AND SUPPORT FOR SECURITY ADMINISTRATORS

The Government of Saskatchewan provides the following services and support to assist the SA in fulfilling their role:

(1) *Security Administrator User Guide* is provided to the SA upon approval of BA's IRIS SA account.
(2) Energy and Resources Service Desk:
1-855-219-9373 (toll-free) or ER.Servicedesk@gov.sk.ca
Monday to Friday, 8:00 AM-5:00 PM CST, excluding holidays