Offender Information System Access

Purpose

To ensure access to QCS core offender information systems are appropriately managed.

Scope

This procedure covers the following core Offender Information Systems:

- IOMS (all variants)
- PTAS
- Reporting Services
- Re-Entry Services (RES)

Responsibilities

Operational Support Services is responsible for implementing appropriate provisions to support the offender information systems from unauthorised access and must:

- ensure appropriate security governance is in place to identify and implement access privileges;
- assist in the development of a culture whereby local managers actively organise access privileges and modifications to be made in a timely manner;
- send an agency wide broadcast message to remind managers to conduct the quarterly review of IOMS access;
- create and maintain Offender Information Systems Access Procedure.

Managers/Supervisors of individual work groups (e.g. within Correctional Centres, Probation and Parole Offices, QCSIG, SMS etc.), **in the Statewide Operations and Specialist Operations Directorates** are responsible for authorising, reviewing, managing and monitoring access in accordance with the Instrument of Delegation for System Access and must:

- authorise access in a timely manner to enable authorised users to perform their identified role;
- determine the need for continuation or modification of user access in a timely manner following role changes, staff terminations and relieving arrangements;
- ensure that user access is removed in a timely manner when the user has resigned, been seconded, dismissed or suspended;
- establish adequate measures to enable monitoring on an ongoing basis and review offender information systems access and use;
- ensure evidence of such reviews is maintained;
- take appropriate steps to develop a culture within work-units for access to be proactively managed;
- communicate any required changes or action updates to access privileges in a timely manner; and
- advise QCS Intelligence Group via email [redacted] of any access requirements, amendments and terminations to IOMS Intelligence module.

DJAG Information Technology Services (ITS) provides:

- Departmental support and controls for ICT security in accordance to DJAG Information Security Policy.
- Policy direction for the use of Information and Communication Technology (ICT) facilities and devices.
- Infrastructure management to facilitate authentication, network logon and access to network resources.

Systems users are required to acknowledge prior to the provision of access that they:

- have read and accepted the responsibilities and conditions on the use of information systems; and
- understand and accept the Department's Information Security Policies and Procedures.

Note: Instrument of Delegation of Systems Access specifies the managers responsible for provisioning of access to offender information systems. It is important to note that some aspects of access, e.g. sentence management services, Intelligence information, parole board can only be approved by the relevant manager of that function. That is, some functions will not be able to be authorised at the local level.

Process

This procedure has been divided into the following sections:

1. Request for access
2. Modify existing access
3. Review of access
4. Removal of access

Note: My IT Service Centre User Guide can provide users with detailed instructions on how to use My IT Service Centre and how to complete access request forms.

1. Request for access

a. Authorised users requesting access to offender information systems covered by this procedure must select, complete and submit the appropriate System Access Request form from *My IT Service Centre*.
b. All access requests must be reviewed, then approved or denied, by a delegate with the appropriate level of authority as per the Instrument of Delegation for System Access.
c. Incomplete System Access Request forms will not be actioned.
d. Unauthorised forms will not be accepted.
e. For IOMS:
    i. IOMS access can only be granted to users with active network access.
    ii. IOMS information assets are classified as Protected and access can only be granted to authorised users.
    iii. IOMS Production users must agree to the IOMS Conditions and Agreements online at the time of request or by completing the IOMS Conditions & Agreement form (PDF 436KB) and attaching to the request.
    iv. Access to other IOMS environments e.g. training can only to be granted to appropriate authorised users, as required.
    v. A delegate may only authorise access for a function for which they have direct responsibility.

2. Modify existing access

a. Managers/Supervisors of work groups must determine the need to modify IOMS access due to agency staff role changes, secondment, and relieving arrangements.
b. To modify existing access to PASS (Provider Access and Service System), complete the appropriate System Access Request form from *My IT Service Centre*, select *PASS Access*, in the *Request Type*, select *replace access or additional access.*
c. To modify existing access to IOMS, complete the appropriate IOMS Access (Production – Blue) form from *My IT Service Centre*, in the *Request Type*, select *Remove Selected Access, Replace existing access* or *Add to existing access*.
d. All access modification requests must be reviewed, then approved or otherwise, by a delegate with the appropriate level of authority as per the Instrument of Delegation for System Access.
e. Incomplete System Access Request forms will not be actioned.
f. Unauthorised forms will not be accepted.

3. Review of access

a. System users and managers are responsible for ensuring that the user's existing access privileges are authorised and commensurate with the current requirements of their role.

b. For IOMS:
    i. A full audit of all users' IOMS access is to be completed annually.
    ii. A quarterly review of access of users whose access has been varied due to changes in their role, e.g. higher duties, secondments, extended leave.
    iii. Offender Information Systems branch is to publish the schedule for IOMS quarterly review in the QCS intranet.
    iv. Offender Information Systems will send email notification to Managers of individual work groups in the Statewide Operations and Specialist Operations Directorates.
    v. Following receipt of quarterly email reminder, Managers / Supervisors of individual work groups in the Statewide Operations and Specialist Operations Directorates must:
        - identify and verify the **active** authorised users within their area have valid and legitimate right to access IOMS and that each user's access rights are commensurate with their current position;
        - utilise the **IOMS User Access by Location** report from Reporting Services reports to assist in the review;
        - ensure that reviews are documented with evidence retained, followed-up if required, and completed each quarter.

4. Removal of access

IOMS access will automatically be removed when user's network access is removed.

The following process is to be followed when requesting IOMS access be removed but keeping the user's network access.

a. Authorised users requesting removal of access to information systems covered by this procedure must select, complete and submit the appropriate System Access Request form from *My IT Service Centre*.
b. For IOMS, complete the appropriate IOMS Access (Production – Blue) form from *My IT Service Centre*, in the *Request Type*, select *Deactivate IOMS Account and Remove All Access.*
c. Unauthorised forms will not be accepted.

Mark Rallings
Commissioner

Last Updated Date: 13/6/2017 Last Reviewed Date: 30/11/2017

Contacts

[redacted]

A/Executive Manager, Systems & Assurance

Offender Information Systems

[redacted]

GPO Box 1054, BRISBANE QLD 4001

Resources

Procedure Properties

Title: Offender Information System Access

Category: Support Services
Version: 03
Implement Date: 27 March 2017
Application: Agency
Availability: In-Confidence

Authority

- Queensland Government Enterprise Architecture (QGEA) information standard:
  - Information security - IS18
  - Use of ICT Services, facilities and devices - IS38
- *Corrective Services Act 2006*
- *Information Privacy Act 2009*

Related Policy Instruments

- DJAG Information Security Policy

Guidelines

- My IT Service Centre User Guide
- QCS Intranet: Forms and Template - Information Systems
- Instrument of Delegation for System Access (IOMS Production)
- IOMS eHub - Access

Attachment

- IOMS Access Request Process Model

Appendices and Forms

- Information Systems Forms
- Instrument of Delegation for System Access
- IOMS User Access by Location
- My IT Service Centre