# PDO INCIDENT MANAGEMENT - PIM

## Quick Reference Guide

<table>
<thead>
<tr>
<th>Document ID</th>
<th>PIM- Roles and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Type</td>
<td>Quick Reference Guide</td>
</tr>
<tr>
<td>Security</td>
<td>Public (PDO users and Contractors)</td>
</tr>
<tr>
<td>Discipline</td>
<td>HSE</td>
</tr>
<tr>
<td>Owner</td>
<td>Nasser AlAmri MSE511</td>
</tr>
<tr>
<td>Issue Date</td>
<td>22 May 2019</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Keywords:** This document is the property of Petroleum Development Oman, LLC.
PDO Incident Management (PIM)

Roles and Responsibilities

**PIM Administrator:** Assigned IM&T person with full control of the application and **responsible for the health and integrity of the system on technical terms including:**

- Trouble shooting and resolution of IT related issues.
- Escalation of technical issues to the vendor and follow-up.
- System enhancements and maintenance including patch upgrades.
- Coordinate implementation of change requests changing

**HSE Global Gatekeeper:** System custodian and representative responsible for ensuring the application is up and running, as per agreed design, to cater for the organizational requirements and have full control over the HSE Modules; responsibilities include:

- Checking PIM application is up and running.
- Reporting issues to PIM Administrator.
- Addressing data issues with owners.
- Producing reports on status of incidents and actions.
- Providing support to PIM end users in progressing their incidents or actions to closure.
- Providing PIM training to end users (class training, user guides, video tutorials, etc).
- Controlling user access levels.
- Checking all new changes introduced in the test server system before they are copied to the Production server.
- Gathering information about new enhancements required by PIM users and performing feasibility studies on the suggestions.

**HSE assurance Gatekeeper:** The person who has full control to the HSE assurance modules and responsible to review Assurance Audits and upload the outcome actions.

**HSE assurance user:** The person who has data visibility to the HSE assurance modules.

**Local assurance Gatekeeper:** The person who has full control to the Local assurance modules and responsible to review Local Assurance audits and upload the outcome actions.

**Local assurance user:** The person who has data visibility to the local assurance modules.

**Environmental Gatekeeper:** The person who has full control to the Environmental incidents and responsible review the corporate Environmental incidents and consequences.

**BCI admin:** The person who has full control to the BCI modules and responsible to enter and review BCI incidents and upload the outcome actions.

**BII admin:** The person who has full control to the BCI modules and responsible to enter and review BII incidents and upload the outcome actions.
**Directorate’s focal point:** A person with higher level authority access to edit specific entries (typically the HSE Team Leaders and/or PIM Focal Points) and responsible to:

- Review new incident entries.
- Review weekly Bundle Report with the below details:
  - Incidents in “Open” and “Pending Final Approval” status.
  - HSE and Assurance Actions in “Open”, “In progress” and “Pending Final Approval” status.
  - Incidents Quality Assurance report.
  - Incident RAM potential.
  - Injury illness report.
- QC and Editing of incidents (e.g. change Responsibilities, adding Attachments, etc.)
- Edit HSE Actions:
  a. Change Target Date, “needs Director Approval”.
  b. Change Action Party, “needs agreement from the new action party”.
- Train, guide and assist their colleagues in “How To” use PIM; assisting PIM users in progressing their incidents or actions to close.
- Liaise with PIM Custodian (MSE51) to raise end users support issues or improvements.
- Periodically attend the incident/RAM review meeting with MSE team to review/discuss the High Potential Incidents within their Directorates

**Incident Module:**

**Entered By:** The person who is entering the incident data into the system (could be the same person who reports the incident). The role is to enter all the mandatory fields in the incident first report and save it as Draft 1. Additional information can be added later to the incident after saving it and then progress the incident to Draft 2 by submitting it to the “Responsible Supervisor”. A maximum of 16 hours is allowed to submit the incident

**Reported By:** The person who reported the incident. This may/may not be the same as the person entering data into the system.

**Responsible Supervisor:** This is the first person to be notified of the event (within 24 hrs), and the person who is responsible for reviewing and validating the data, assessing the risk, and making assignments for and completing consequence information.

The system will automatically assign him/her as incident owner. So, if it needs to be changed to another person, then he/she can do that by changing the incident owner field and progress the incident by submitting it to the new incident owner within 3 days of the incident.

If the initial Responsible Supervisor is not the correct person, then he/she immediately should find out who is the right person and change the “Responsible supervisor” and “Incident Owner” fields under in the responsibilities tab.
**Incident owner:** The person who owns the incident and accountable to progress the incident until complete closure and responsible to:

- Make sure that all relevant fields are selected, updated and accurate
- Assign actions, where needed, and follow up to close them.

**Incident approver:** The person who does the final review of the incident and ensures:

- All documentations have been attached.
- Investigations, consequences and the actions have been closed.
- If it is required, reject the incident and send it back to the incident owner.

**Notify Only:** A person or group of people who need to be aware about the incident but have no role to progress the incident to closure.

**Action Item Module:**

- **Entered By:** The person who is entering the action(s) in the PIM.
- **Assigned By:** The person who is assigning the action to the “Action Party” needs to agree with the action party before assigning the action. He/she could be the same person entering the action in PIM.
- **Pre-Action Approver:** The person who approves the action before sending it to the “Action Party”.
- **Action Party:** The person who is responsible to complete the action and send it to the “Post Action Approver” to approve the action taken and close it.
- **Post Action Approver:** The person who verifies the action taken. He/she can reject and send it back to the “Action Party” justifying the rejection otherwise he can approve and close the action if it meets the requirement.