



Power to Ontario.
On Demand.

**Meter Data Management and
Repository (MDM/R)**

**Incident Management
Manual**

Issue 0.95

This document provides an overview of the responsibilities of MDM/R service recipients making use of the MDM/R incident management framework set out in the MDM/R Terms of Service.

MANUAL

Disclaimer

The posting of documents on this Web site is subject to the terms and conditions posted on the SMSIP Web site. Please be advised that, while the *IESO-SMSIP* 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.

DRAFT

Document ID	SME_MAN_0007
Document Name	Incident Management Manual
Issue	Issue 0.95
Reason for Issue	New revisions for further comment
Effective Date	June xx, 2011

Document Change History

Issue	Reason for Issue	Date

Related Documents

Document ID	Document Title
SME_AGR_0002	<i>MDM/R Terms of Service</i>
SME_AGR_0001	<i>SME-LDC Agreement</i>
SME_PRCs_0001	<i>MDM/R Temporary Change Control Process</i>
SME_MAN_0006	<i>MDM/R Change and Baseline Management Manual</i>

- intentionally left blank-

DRAFT

Table of Contents

Table of Contents	i
List of Tables	ii
Table of Changes	iii
1. Introduction	1
1.1 Scope	1
1.2 Who Should Use This Document.....	1
1.3 Assumptions and Limitations	1
1.4 Conventions	1
1.5 Roles and Responsibilities.....	2
1.6 How This Document Is Organized	2
2. MDM/R Service Desk	3
3. Incident Management Process	5
3.1 Incident Management Overview	5
3.2 Guiding Principles.....	5
3.2.1 <i>Incident Life Cycle</i>	6
3.3 Incident Management Activities and Expectations	8
3.3.1 Incident recording and notification	8
3.3.2 Incident support and priority classification.....	9
3.3.3 Investigation and diagnosis.....	11
3.3.4 Recovery and Resolution.....	13
Incident Tracking, Communication, and Escalation.....	15
3.3.5 Incident Closure.....	15
3.3.6 Incident Monitoring	16
3.4 Major Incident.....	17
3.5 Incident Classification Criteria.....	17
3.5.1 Priority Classification	17
3.5.2 Incident Response and Resolution Operating Level Targets.....	19
4. Service Request Management	21
References	22

List of Tables

Table 3-1 – Impact Classification Question 18

Table 3-2 – Urgency Questions..... 19

Table 3-3 – Priority Calculation 19

Table 3-4 – Incident Response and Resolution Targets20

DRAFT

Table of Changes

Reference (Section and Paragraph)	Description of Change

DRAFT

- intentionally left blank-

DRAFT

1. Introduction

This manual is part of a series of documents (the MDM/R Manuals and Procedures) that detail the interactions required between the Smart Metering Entity (SME) and the MDM/R service recipients in using Meter Data Management Repository (MDM/R) services.

The MDM/R Manuals and Procedures are enabled by contractual agreement (the “SME-LDC Agreement” or any other instrument that binds the MDM/R service recipient to the “*MDM/R Terms of Service*”) between the SME and the MDM/R Service Recipient – subject to those documents being put into legal force. In the interim, this manual may be further referenced by other legal instruments pertaining to the relationship between the IESO and a given MDM/R service recipient where applicable.

The procedures described in this manual satisfy the obligations described in the MDM/R Incident Management Framework portion of the *MDM/R Terms of Service*.

1.1 Scope

The processes captured within this manual define the MDM/R Incident Management process. The Incident Management process defines how Service Recipients and the SME work together to record, classify, and manage incidents to restore service, and to fulfill pre-approved service requests.

The Incident Management Process may also trigger other MDM/R processes and/or internal SME procedures, including but not limited to Problem Management, MDM/R Business Continuity, and Change Management.

This procedure does not include the procedures for the resolution of incidents or problems that are determined to be caused by or within the MDM/R service recipients’ systems or processes. These remain the responsibility of the MDM/R service recipient to resolve.

1.2 Who Should Use This Document

MDM/R service recipients who have signed the *SME-LDC Agreement* or have otherwise commenced production operations with the MDM/R under the applicable framework which gives relevance to this document.

1.3 Assumptions and Limitations

This manual pertains to incidents and problems and the extent to which those incidents are within the scope or responsibility of the MDM/R Operational Service Provider (OSP – see section 1.5 “*Roles and Responsibilities*” below.).

1.4 Conventions

For the purposes of this document, any references to “IESO” or the Smart Metering Entity (“SME”)

may be construed to mean the same entity.

For the purposes of this document, any references to “MDM/R service recipient” shall be considered to include the principal party (i.e. the local distribution company), authorized Advanced Metering Infrastructure (AMI) Operators and Billing Agents of the *MDM/R service recipient*.

1.5 Roles and Responsibilities

The SME shall be *responsible* for providing the overall management and administration of the Incident Management process. The SME will be the principal point of contact with MDM/R Service Recipients in this regard.

The MDM/R Operational Service Provider (OSP) has direct responsibility, by way of a separate agreement with the SME, over the operation of the MDM/R in accordance with established service levels. References to the MDM/R OSP in this document are used to help explain the flow of events over the incident lifecycle. However, as will be explained in this document, the IESO maintains primary responsibility to manage the incident management process.

The MDM/R Service Recipient shall be responsible for internal analysis of incidents prior to contacting the SME to ensure the incident is not internal to their organization. The MDM/R service recipient shall also be responsible for providing relevant additional detail and information when requested by the SME or the OSP as per this manual.

The MDM/R service recipient shall be responsible for the resolution of incidents and problems determined to be caused by their systems and/or processes, including but not limited to sending data to correct the incident or problem.

1.6 How This Document Is Organized

- **Section 2** provides an overview of the nature and role of the MDM/R Service Desk.
- **Section 3** provides an overview of the incident management process as offered by the MDM/R Service Desk.
- **Section 4** provides an overview of the service request management process as offered by the MDM/R Service Desk.

– End of Section –

2. MDM/R Service Desk

The objective of the MDM/R Service Desk is to act as a central point of contact between MDM/R service recipients and the SME and OSP in the operation of the MDM/R, to handle incidents and service requests.

The SME Service Desk is responsible for:

- Providing Tier 1 support to Service Recipients;
- Logging all relevant incident and service request details;
- Ensuring all relevant incidents and service requests are properly recorded, classified and prioritized;
- Providing initial assessment of all incidents: make first attempt at Incident resolution and/or refer to 2nd line support, based on defined operating level targets;
- Resolving incident and /service requests they are able;
- Monitor and escalate incidents to other support tiers according to agreed operational level targets;
- Monitoring resolution of incidents to help ensure they are resolved within defined operational level targets;
- Keeping MDM/R Service Recipients informed on status and progress;
- Closing all resolved incidents, request and other calls;

Support tiers that the SME Service desk may work with in resolution of an incident ticket include:

- Tier 2 – OSP Support provided by the SME Service Provider; and,
- Tier 3 – Vendor Support provided by the various third party vendors that may have provided application or hardware components that make up the MDM/R System.

The MDM/R Service Desk can be accessed through the:

- Self-Service Portal;
- Email; and,
- Phone.

Self-Service Portal:

The preferred method of communication for recording new Incidents or making a Service Request is through the web self-service interface to the Incident Management System. Self-service forums allow for direct submission into the Incident Management System for review, classification, and prioritization by the SME. The Web Self-Service tool provides Service Recipients with easy access to the latest Service Desk information and services including features to:

-
- Record and open new incidents;
 - Request new service requests;
 - Review, update, monitor, and close existing Incidents opened by your organization;
 - Review, and monitor Incidents affecting all users of the MDM/R system;
 - View known errors or problems identified within the Production environment or System Releases being evaluated and tested for production in one of the development environments; and,

Access to the Self-Service Portal is governed by the contacts your organization has provided us through the submission of the MDM/R Organization Contacts (SME_FORM_0004) form. Any contact identified as either an 'Incident and Notification' or 'Full Access User' will be granted a User ID and password to access the Self-Service Portal.

- 'Incident and Notification' contact types will have the ability to create, modify, and review all tickets associated with the Service Recipient via the Self-Service portal.
- 'Full Access User' contact types will have the same ability as the 'Incident and Notification' contact type AND will have the ability to deactivate users, for your LDC, within the Self-Service Portal. Please note, this deactivation only applies to access to the Service Desk Self-Service Portal. It does not apply to the MDM/R Graphical User Interface (GUI).

Email

Email can be used to respond to, update, or escalate existing Incident or Problem records opened in the Incident Management System. Email can also be used for raising clarification questions.

Phone

The phone can also be used to reach the Service Desk to raise, monitor, update, and escalate Incidents or Service Requests.

Service Recipients may use the phone in addition to email or web self-service communications to alert or escalate high severity or urgent incidents and requests.

– End of Section –

3. Incident Management Process

3.1 Incident Management Overview

An incident is defined as an unplanned interruption to an MDM/R service or reduction in the quality of an MDM/R service.

Incident Management is the process for dealing with all incidents to restore normal service operation as quickly as possible and to minimize the adverse impact on MDM/R service recipient business operations, thus ensuring that defined service quality and service levels are maintained.

Incident Management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by MDM/R Service Recipients or the SME either through the MDM/R Service Desk, Self-Service Portal, email, or phone.

Service restoration includes restoring system services to the on-line state as well as the catch-up of back logged data processing activities in order to return the system to normal service level operations.

The intent of this section is to define the MDM/R Incident Management process including:

- Guiding Principles
- Incident Life Cycle
- Incident Management Activities
 - Incident Recording and Notification
 - Incident Support and Priority Classification
 - Investigation and diagnosis
 - Recovery and Resolution
 - Closure
 - Incident Monitoring
- Incident Classification Criteria
- Target Incident Response and Resolution Times

3.2 Guiding Principles

The SME and Service Recipients both play active roles in the identification, recording, classification, and resolution of Incidents. The SME and Service Recipients will conduct Incident Management activities consistent with the following guiding principles:

- Commitment and focus to reducing the impact of all incidents by their timely resolution within expected, contracted, and targeted timelines.
- All incidents should be managed in conformance with the procedures documented within this manual.
- Wherever possible, the MDM/R Service Recipient will be provided with the means to continue their billing and business functions, even if via a degraded service.
- In scenarios where an incident has impacted the ability of the MDM/R system to provide the expected system output as part of any MDM/R service used by the MDM/R Service Recipient and a manual work around is required, the SME and OSP will make commercially reasonable efforts to ensure that the output of the manual workaround is consistent with the

specified and expected format such that impacts to downstream MDM/R Service Recipient processing are minimized.

- The SME shall advise MDM/R Service Recipients of incidents where the completeness, quality, or format of system output has been affected.
-
- If required and where possible the SME will make reasonable efforts to work with MDM/R Service Recipients to establish an appropriate work around to recover service.
- MDM/R Service Recipients will make commercially reasonable efforts to investigate and correct incidents and problems stemming from their systems and processes to reduce their re-occurrence and impact to the operability, performance, and availability of MDM/R services.

3.2.1 Incident Life Cycle

There are many states that an Incident ticket goes through as it is managed by the SME to closure. Figure 3-1 below illustrates the key Incident states relevant to MDM/R Service Recipients. Incident tickets may be assigned to multiple SME support users and additional states within the Incident Management System exist to assist the SME in managing incident tickets to closure through the various MDM/R support tiers.

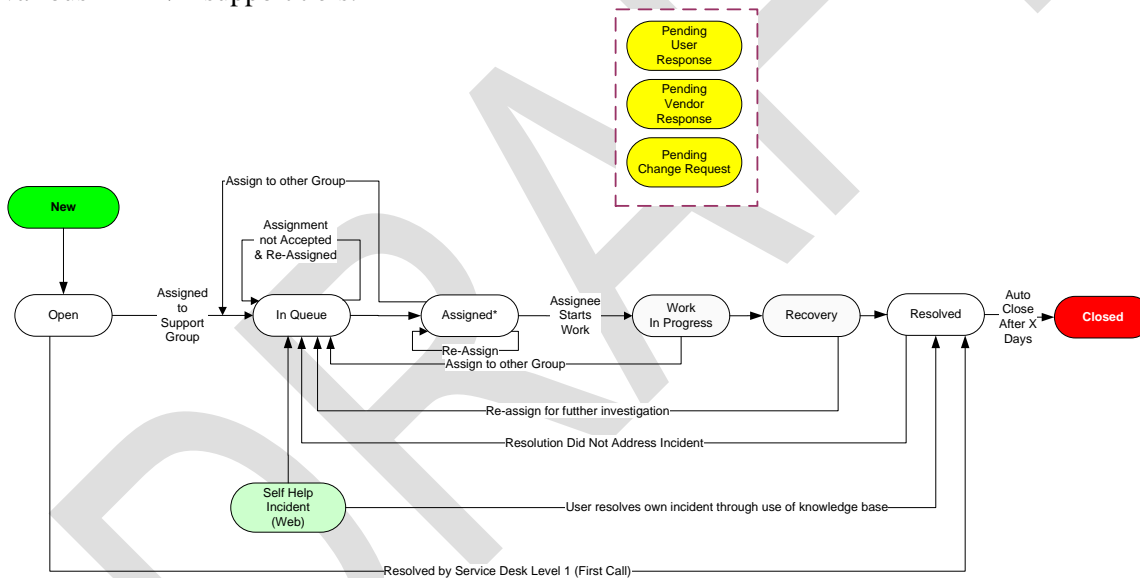


Figure 3-1 – Incident State Diagram

New

All incident tickets are assigned the state of 'new' upon creation. Incidents will stay in this state until their initial review by the Service Desk.

Open

A state of 'open' indicates an incident ticket is undergoing its initial assessment by the Service Desk.

In Queue

A state of 'In Queue' indicates the Service Desk has completed the initial assessment of the incident ticket and the ticket has forwarded to a specific group for further investigation and is awaiting assignment to a subject matter expert within the group.

Assigned

A state of 'assigned' indicates the incident ticket has been assigned to a subject matter expert for further evaluation.

Work In Progress

A state of 'work in progress' indicates the incident ticket has been accepted and is currently being investigated by a subject matter expert.

Recovery

A state of 'recovery' indicates that the steps required to resolve the incident have been identified and communicated but not yet completed. Once the recovery steps have been completed, the incident status will transition to 'resolution'

Resolved

A state of 'resolved' indicates that the recovery steps have been completed and that the incident has been remediated. Unless objection is received from the ticket originator, the incident status will then transition to closed after a defined period of time.

Closed

A state of 'closed' indicates the incident ticket has been resolved and that no further actions are required.

Pending User Response

A state of 'pending user response' indicates the Service Desk is waiting for information from the ticket originator before proceeding with the incident investigation and analysis.

Pending Vendor Response

A state of 'pending vendor response' indicates the Service Desk is waiting for information from the vendor before proceeding with the incident investigation and analysis

Pending Change Request

A state of 'closed' indicates the Service Desk is waiting for a change to be initiated via the change request process prior to resolving the incident ticket.

3.3 Incident Management Activities and Expectations

The intent of this section is to define the key Incident Management activities between the SME and MDM/R Service Recipient in identifying, recording, alerting, classifying, investigating and resolving MDM/R Incidents. The key Incident Management activities are defined below and for each, expectations of both the SME and MDM/R Service Recipients are outlined.

Throughout the incident management activities, the SME will provide MDM/R Service Recipients a facility through the Service Desk Self-Service Portal to:

- View and extract all current and historical incident records impacting the MDM/R Service Recipient that were opened by the MDM/R Service Recipient organization, an individual user within the MDM/R Service Recipient organization, or the SME.
- Extract or report on information on incidents at detailed or summary level by pre-defined or configurable time period including incident type, impacted service, category, impact, urgency, target resolution (“resolve”) time and actual resolution (“resolve”) time.
- Provide additional information as required through the life cycle of the incident. MDM/R Service Recipients may be re-assigned incident tickets or be requested to provide further updates during Incident Investigation and Diagnosis, and during Incident Resolution and Recovery

3.3.1 Incident recording and notification

Description:

All incidents shall be recorded in terms of symptoms, basic diagnostic data and information about the service(s) affected. Incidents can be identified by both the SME and MDM/R Service Recipients.

- On the basis of the priority and the Target Response and Recovery Times or where applicable, SLA, the affected MDM/R Service Recipients will be informed about the estimated target time to resolve the incident, and when updates on progress will be available.
- The SME will always endeavor to explicitly outline in initial alerts to MDM/R Service Recipients whether or not there is a possibility that the format, completeness, or quality of output files may have been affected by the incident.

MDM/R Service Recipient Expectations

- Service Recipients will review current open Incidents and Known Errors on the Service Desk Self-Service Portal in advance of reporting new Incidents such that the MDM/R Service Recipient can suggest whether or not it is believed there is a match against an existing incident.
- Service Recipients will request SME assistance in working around a Known Error or Problem by opening a new Incident record for the new occurrence of the Known Error.
- Service Recipients will record all incidents regardless of whether or not they are Known Errors such that the appropriate monitoring and trending may occur in support of Problem Management process.
- Service Recipients will make best efforts to provide all of the details required to enable the SME and OSP to adequately investigate the ticket. If the Service Recipient does not provide enough detail to identify the USDP or investigate the incident behaviour as reported and the SME is required to request further detail from the Service Recipient, the Service Recipient is

expected to respond within the defined Service Recipient response timelines based on classified incident priority.

- Service Recipients will assign an incident owner if the ticket is opened by the SME. Service Recipients will have the appropriate Incident Management processes in effect such that Incident notifications sent to Service Recipients are responded to by the Service Recipient to provide the SME with the Service Recipient Incident Owner within the defined Service Recipient response time. The Service Recipient user that replies to the Incident Notification email is automatically assigned as the owner by the Incident Management System.
- Service Recipient will review initial Incident classification criteria and calculated priority. If the priority classification of the incident is not consistent with the impact and urgency definitions outlined in this document, the Service Recipient will contact the SME to discuss escalating or lowering the existing incident priority. The Service Recipient will be able to dispute initial incident classification by:
 - Responding to the SME Incident Notification email; or,
 - Calling the SME Service Desk.

Smart Meter Entity (SME) Expectations

- The SME will record all incidents regardless of whether or not they are initially determined to affect Service Recipients. This includes re-occurrences of ‘known errors’ or problems.
- Incidents that are determined to affect Service Recipients will be communicated to Service Recipients within the time periods defined in this document.
- Where it is assessed as likely that quality, completeness, or format of any output files could have been impacted by the identified incident, the SME will inform Service Recipient(s) as part of the initial incident notification so that precautionary measures can be taken where deemed necessary to halt downstream processing until the incident can be further assessed and diagnosed.

SME/OSP Initiated Incident Notification Criteria

The SME/OSP must log and notify Service Recipients if any event that is consistent with the definition of an incident occurs except when the incident is determined to not affect standard operation of a service or a reduction in the quality of service to Service Recipients. Incidents that don't affect Service Recipients directly should be logged in the Incident Management System to support Problem Management; however, are not required to be reported out to Service Recipients. If it is unclear whether or not the incident affects Service Recipients, the SME will notify Service Recipients.

An example of an incident that doesn't affect Service Recipients may include failure of a redundant application server that doesn't affect or degrade quality of service in production or the ability to successfully fail over to a secondary operating site in a Disaster Recovery event.

3.3.2 Incident support and priority classification

Description

Incident records raised should be analyzed to discover the reason for the incident. Incidents should also be classified, and it is the classification system determines the priority of further resolution actions.

- Incident support and priority classification will initially occur as part of opening the incident ticket.
- Detailed classification will be completed by the SME Service Desk with the aim of determining the incident category to facilitate monitoring and reporting.
- The criteria defined within the manual will be used for the classification of MDM/R Incidents.
- Incident priority will take into consideration both impact of the incident to Service Recipients as well as urgency.

Service Recipient Expectations

- The Service Recipient will confirm SME classification of Incident priority. When Incident notification is first received for incidents identified and initially opened by the SME, Service Recipients are responsible for reviewing the incident and confirming the defined priority classification.
- The Service Recipient shall attach all relevant and supporting artifacts to the Incident Record when it is first opened to support investigation and diagnosis by the SME.
- The Service Recipient, where required, will provide additional detail to support investigation including where necessary, supporting interface files to support incident diagnosis.
- The Incident Management System will have the ability to re-assign incident tickets back to the Service Recipient Incident owner and track the Incident Owner response time during this period. The Incident Management System must also be able to calculate the total time added to the Target Recovery Time due to delay in Service Recipient provision of supporting incident detail and artifacts.

SME Expectations

- The SME will apply the classification of Incident priority based on the criteria established in this manual.
- The SME will investigate the incident and categorize further to facilitate monitoring, reporting, and triage to the appropriate support tier for investigation and diagnosis if the incident cannot be traced to a 'known error'. SME classification should include:
 - Incident Category – Incidents should be assigned to a category on the basis of the suspected origin of the incident or relevant support group.
 - Service – Services impacted by the incident should be captured on the incident record with reference to the applicable SLA. E.g – If the incident is identified as impacting a critical service, the SLA associated with Target Resolution Time should be consistent with the requirements outlined in this manual.
 - Support Group – If the Service Desk cannot solve the incident within predefined timescales, it is determined which support group should deal with the incident.
- The SME should associate new incidents with known incidents or problems where they are related.

Priority Disagreements

- If Service Recipients do not agree that the priority classification calculated by the Incident Management System does not adequately take into consideration impact to the Service Recipient or urgency, Service Recipients will be able to request an adjustment to the priority of the incident as follows:
 - To request an increase in priority, Service Recipients should note this request within the ticket. To escalate priority, Service Recipients should be able to objectively outline based on defined incident classification criteria why the incident priority should be escalated.
 - The SME should consider the request and make reasonable efforts to escalate incident priority where feasible until incident Investigation and Diagnosis is complete.
 - The SME is able to override initial priority determination once Investigation and Diagnosis is complete. If after investigation and diagnosis is complete, the SME believes the incident priority should be downgraded, the SME may update the priority in the incident ticket, but must document within the Incident record the justification for downgrading the incident based on defined incident classification criteria. When the incident record is updated to revise incident priority, affected Service Recipients must be notified of the change.
 - If after incident Investigation and Diagnosis, the Service Recipient disagrees with the priority assessment, the Service Recipient may again escalate to the SME. The SME will have the final decision on Incident Priority; however, where the SME disagrees with a Service Recipient escalation request after Investigation and Diagnosis and upon request from the Service Recipient, the SME will respond with the rationale for the SME's assessment.
 - . If the Service Recipient is still in disagreement regarding the decision, further escalation can be made to the SME Steering Committee that represents Service Recipients.

3.3.3 Investigation and diagnosis

Description

If there is no known steps to recover from the incident the incident is then investigated. The Service Desk routes incidents, for which no immediate solution is available or which go beyond their expertise, to an appropriate SME and/or OSP support group. This support group will then investigate and diagnose incident, or route it to another support group. The Service Desk is responsible for ensuring that investigation and diagnosis is completed within operational targets and escalating incidents where applicable.

The investigation and diagnosis should consider the balance between restoration of service and implications to data integrity and downstream Service Recipient processing.

Service Recipient Expectations

- Service Recipients are expected to make available, when necessary, the appropriate support staff to help evaluate resolution alternatives including proposed incident workarounds necessary to restore service.

SME Expectations

-
- SME diagnosis of Incidents will include an understanding of the MDM/R services affected by the incident and diagnosis.
 - The SME and applicable support groups will investigate and diagnose what has gone wrong or being sought by the Service Recipient, understanding the chronological order of events, confirming the impact of the incident, identifying any events that could have triggered the incident (eg. A recent change, some Service Recipient action), knowledge searches for previous occurrence by searching previous incident/problem records, error logs or other knowledge bases.

DRAFT

3.3.4 Recovery and Resolution

Description

This step identifies potential solutions to address the incident. When a potential solution has been identified, it should be applied and tested.

Specific actions to be undertaken and the people involved in the recovery actions may vary depending upon the nature of the fault, but could involve:

- Asking the Service Recipient to undertake directed activities on their own environment
- The SME implementation of the resolution for all Service Recipient or for each affected Service Recipient
- Specialist support groups being asked to implement specific recovery actions.
- Third-party supplier or maintainer being asked to resolve the fault.
- When resolution has been found, sufficient testing must be performed to provide reasonable assurance that recovery action is complete and that MDM/R service has been restored.

Wherever possible, the proposed solution should consider that Service Recipient be provided with the means to continue their billing and business functions, even if via a degraded service. Commercially reasonable efforts should be made to minimize the impact of the incident on the Service Recipient and to provide more time to investigate and devise a structural resolution.

After successful execution of the resolution or circumvention activity, service recovery actions can be carried out.

The Incident Management System will allow the recording of events and actions during the resolution and recovery activity.

For some solutions, a Request For Change (RFC) will have to be submitted to Change Management. The Change Management process is initiated any time a system change is required to resolve an incident. Please refer to the Change Management Manual.

SME Expectations

- The SME, where appropriate and based on assessed level of risk, is expected to perform reasonable testing of system changes, scripts, data repairs or any other workaround mechanism that may be implemented which manipulates Service Recipient data or affects the functional characteristics of the MDM/R system.
- The SME will make reasonable efforts and where feasible to provide the opportunity for the affected Service Recipient or representative from the group of affected Service Recipient(s) to be involved in assessing the proposed resolution approach when the incident is identified as having implications to the completeness, quality, format, and availability of data made available and required for downstream processing by the Service Recipient. The SME will balance the need to restore service as soon as possible and implications to one or multiple Service Recipients' downstream processing.
- The SME and OSP will make reasonable efforts and where it is possible to produce output of a manual workaround that is consistent with the specified and expected format such that impacts to downstream Service Recipient processing are minimized in scenarios where an incident has impacted the ability of the MDM/R system to provide the expected system output as part of any MDM/R service used by the Service Recipient and a manual work around is required. Where the completeness, quality, or format of system output is identified as impacted in any way, the SME will advise the affected Service Recipients. The SME will

make reasonable efforts and where it is feasible to jointly work with affected Service Recipients to establish an appropriate work around to recover service or from the incident.

Temporary Fixes

- During the resolution process, it may be necessary to develop a temporary fix or emergency fix. In many cases the temporary fix utilized may form the basis of a temporary work around associated with the Problem. If a temporary fix requires modification of the infrastructure, system hardware or software, then an RFC will have to be submitted first (before the root cause has been determined). If the matter is very serious and delay is unacceptable, the urgent or emergency RFC procedure may be exercised.

Temporary Workarounds

- For incidents matched with 'known errors' being managed within the Problem Management process and that require an SME workaround to be executed, the SME will co-ordinate the implementation of the workaround with Service Recipients if applicable.
-
- For incidents that require a workaround to be established to provide Service Recipients with expected data output, return to a normal data operating state, or any other reason as part of the restoration of service, and the incident cannot be traced to an existing Known Error or problem record, the SME will initiate the Problem Management process in parallel where the workaround details will be captured.

Service Recipient Expectations

- Service Recipients will be available for consultation on the incident, resolution alternatives, and to support validation/testing and implementation actions to recover from the incident and/or restore service.

Incident Tracking, Communication, and Escalation

Incident Tracking

Procedures need to be in place to provide reasonable assurance the incidents are resolved within operational targets.

The SME will provide monthly reporting on Incident Management process key performance indicators to the SME Steering Committee.

Incident Communication – SME Expectations

- The SME will provide email notifications regarding MDM/R incidents to the Service Recipient Incident Owner when:
 - The incident moves through the following states within the Incident Management System:
 - Work-In-Progress – Intended to notify the Service Recipient Owner that the Incident has been assigned and that work has started to diagnose and resolve the Incident.
 - Resolved - Intended to notify the Service Recipient when the Incident has been considered Resolved and the SME is awaiting confirmation that the incident record may be closed.
 - Anytime Service Recipient input is required which could occur when:
 - Further information is required for the SME to properly classify and diagnose the incident or the incident record is assigned back to the Service Recipient Owner;
 - Service Recipient input is required regarding a proposed resolution path.
 - Service Recipient confirmation is required for incident record closure.
- Any time Service Recipient input is required, the SME will define the activity required of the Service Recipient and the target response time that the SME or support groups require a response by.
- Operating Level Targets will be defined by Incident priority.

Incident Escalation

Service Recipients may request escalation of any issue to the Service Desk. Second level escalations of incidents should go to the SME Operations Lead.

3.3.5 Incident Closure

The Service Desk should obtain information to help ensure that the incident has been resolved, and provide opportunity to Service Recipients to confirm that the incident can be closed.

Incidents are considered resolved when service has been restored including processing of any backlogged data and execution of any work around required to re-establish lost data or system output that may have occurred as a result of the incident.

Once the incident is believed to be resolved and the incident record has been appropriately updated to reflect the resolution approach and status, the SME will notify the Service Recipient owner. The Service Recipient will have 5 calendar days to raise any concerns to the SME regarding closing the incident ticket. The Service Recipient Incident Owner may re-open the incident ticket by re-assigning back to the SME and thus changing the state from 'Resolved' to 'Assigned'. If the Service Recipient Incident owner does not respond or provide any feedback to the SME within 5 calendar days, the proposal to close the incident is considered accepted and the incident ticket will automatically move to the 'Closed' state. Once closed, the incident record cannot be re-opened.

At the closure of an incident the root cause of the incident may not be known. The Problem Management process will be initiated to further investigate root cause, and manage the problem associated with the incident. Problem Management, at a minimum, will be initiated in the following scenarios:

- All Priority 1 and Priority 2 incident records opened which cannot be linked to an existing problem or known error.
- Any incident where by a work around to restore service, or affecting the quality, completeness, and format of data used by a Service Recipient.

Where an incident that cannot be traced to an existing Known Error or Problem is closed and a new problem ticket is not opened, the rationale for not doing so will be documented within the Incident ticket.

3.3.6 Incident Monitoring

The Service Desk is responsible for overseeing the resolution of all outstanding incidents whatever the initial source. Incidents and Service Requests that are outstanding past their calculated target time to resolve should be identifiable to the Service Recipient and SME within through the Service Desk Self-Service Portal and the Incident Management System.

Incidents and Service Requests that are assigned to the Service Recipient and are pending Service Recipient input should be identifiable to the Service Recipient and SME within the Service Desk Self-Service Portal and the Incident Management System.

3.4 Major Incident

A 'Major' Incident is defined as any incident that meets the criteria outlined within the Business Continuity Manual as a Yellow Alert or Red Alert; The operational state in which an incident is monitored and assessed for possible activation of business MDM/R disaster recovery plans. The Business Continuity Manual will define the process for an incident upon declaration of a Yellow or Red Alert

3.5 Incident Classification Criteria

When several incidents are being dealt with at the same time, priorities have to be set. These priorities are based on the seriousness of the error to the Service Recipient(s) business including: operational user impact, billing and other business process impact, and reputation. In consultation with the Service Recipient, and in accordance with the provisions of the SLA or expected Target Response and Resolution timelines, the Service Desk assigns the priority which determines the order in which incidents are dealt with. When incidents are escalated to second-line (tier two) or higher level support, their priority is maintained or may be adjusted in consultation with the Service Desk and Service Recipient. Priority is established based on the combination of:

- Impact of the incident – extent of the deviation from the normal service level, in terms of the number of Service Recipient users, customer bills, or business processes affected. Major Incidents are those for which the degree of impact on the Service Recipient community is extreme. Incidents for which the timescale of disruption – to even a relatively small percentage of users – becomes excessive should also be regarded as major; and,
- Urgency of the incident – the speed of response and resolution required considering the length of delay that is acceptable to the Service Recipient business user or business process in resolving the incident.

The tables in the sections below define the criteria used to establish Incident impact and urgency classification.

3.5.1 Priority Classification

When process to create tickets within the MDM/R Service Desk and Incident Management Systems requires a number of questions to be answered. These questions are used to determine the impact and urgency of the incident. Each question has a number of potential answers with each answer awarded a number of 'points' The impact and urgency ratings are determined by summing the impact points from the answers to the impact and urgency questions respectively. Once the urgency and the impact have been determined, the overall Incident priority will be established based on the sum of the impact and urgency points.

Table 3-1 illustrates the current impact question while Table 3-2 illustrates the current urgency questions with the 'points' assigned to each potential answer. The questions, answers, and points

awarded to each answer is configurable and will be periodically reviewed and modified to incorporate MDM/R Service Recipient feedback..

IMPACT QUESTIONS			
Number	Question	Answer	Points
1	Environment Affected	Production	8
		Sandbox	0
		Enrolment (QA)	0
		Sandbox 2 (internal only)	0
		Production Support (internal only)	0
		Training (internal only)	0
2	Functionality Affected	Infrastructure	10
		Synchronization	6
		Meter Read Processing	6
		Graphical User Interface	6
		File Transfer Services	6
		Billing	6
		Web Services	3
		VEE	3
		Framing	3
		USDP ID Generation	2
		Reports	2
		IVR	1
		3	Volume of SDPs affected
Entire population	8		
100 - 10,000	6		
10 - 100 SDPs	2		
< 10 SDPs	1		
4	Multiple ORGs affected	Yes	6
		No	1
		Unknown	2

Table 3-1 – Impact Classification Question

URGENCY QUESTIONS			
Number	Question	Answer	Points
1	Is a workaround available	No workaround available	5

URGENCY QUESTIONS			
Number	Question	Answer	Points
		Yes, acceptable for a limited period	3
		Yes, very acceptable to affected users	1
2	Impact of Delay	Critical – Immediate turnaround is requested	8
		High – Quick turnaround is requested	6
		Medium – Default urgency level	4
		Low – Low urgency	2
3	Is this a recurring issue	Yes	3
		No	1
		Unknown	2

Table 3-2 – Urgency Questions

Table 3-3 below illustrates how the priority is assigned using the total of the impact and urgency points.

PRIORITY CALCULATION	
Total Points	Priority
0 to 9	5
10 to 21	4
22 to 29	3
30 to 35	2
36 and over	1

Table 3-3 – Priority Calculation

3.5.2 Incident Response and Resolution Operating Level Targets

The SME and Service Recipients will perform MDM/R Incident resolution activities within the timelines defined in this section.

Priority	Clock	Initial Response Time	Time to Recovery	Time to Resolution
1	24x7	30 min (1 hr)	N/A	24 hrs

2	Business Hours	1 hr	1 business day	2 business days
3	Business Hours	3 hrs	2 business days	5 business days
4	Business Hours	2 business days	3 business days	10 business days

Table 3-4 – Incident Response and Resolution Targets

Initial Response Time

The Incident Response Time is defined as the target it time it takes for the SME to respond and acknowledge a new incident. An incident is considered responded to when it has been set to the ‘Open’ state within the Incident Management System.

Time to Recovery

The Time to Recovery is defined as the elapsed time starting when the incident is first identified and recorded to the time that the incident has been fully assessed and the scope of the incident diagnosed and recovery steps identified.

Time to Resolution

The Time to Resolution is defined as the elapsed time starting when the incident or service request is first identified and recorded to the time that the incident is moved to the ‘Resolved’ state in the Incident Management System.

– End of Section –

4. Service Request Management

The purpose of the Service Request Management is to:

- Provide a channel for Service Recipients to request and receive standard services for which a pre-defined approval and qualification process exists
- Provide information to Service Recipients about the availability of services and mechanism for requesting the service
- Source and deliver the components of the requested standard services
- Provide general information about the MDM/R services, and may include responses to frequently asked questions.

Service Request Management is the workflow, events, and processes that enables a Service Request to be reliably submitted, routed, approved, monitored and delivered. Incident Management handles the complete Service Request lifecycle from submission through delivery and follow-up.

The Service Request Management function will allow for:

- Classifying and processing Service Requests;
- Request Fulfillment;
- Request Tracking; and,
- Request Escalation and Communication.

Service requests can be made for 'standard services': that are agreed to be provided under agreed timing guidelines; and where records are maintained. Service requests do not pertain to requests made for resolution of a break/fix or data incident.

Examples of Service Requests include:

- Ad-hoc report request
- Non-production environment configuration change
- Data processing inquiry
- Ad-hoc data extract
- Data query request
- User access and/or change request
- Support question
- Organizational documentation change

Individual Service Requests will be configured within the Incident Management System as they are identified through operational experience and approved through the Change Management process. When a new type of MDM/R Service Request is identified, it will be added to the Service catalogue and a request specific work flow will be established to make the request.

References

Document Name	Document ID
<i>MDM/R Terms of Service</i> – NOT IN FORCE	SME_AGR_0002
<i>SME-LDC Agreement</i> – NOT IN FORCE	SME_AGR_0001
<i>MDM/R Temporary Change Control Process</i>	SME_PRCs_0001
<i>MDM/R Change and Baseline Management Manual</i> – NOT IN FORCE	SME_MAN_0006

– End of Document –