

IDA_NEMO_FAL_02-PMB Incident Management

Version	1.1	
Date	22/01/2025	
Status	<input type="checkbox"/> Draft	<input checked="" type="checkbox"/> Final

Previous versions

Version	Date	Author	Summary of changes
1.0	23/05/2024	████████	Version for IDA GL.
1.1	01/01/2025	████████	2.1: Contact details added

Table of Contents

- 1. Introduction 3
 - 1.1. Purpose 3
 - 1.2. Governed / Regulated by 3
 - 1.3. Previous and next procedures..... 3
- 2. Procedure 3
 - 2.1 Overview 3
 - 2.2 Communication with the [REDACTED] Provider during the MCS..... 5
 - 2.2.1. The [REDACTED] encounters the incident 5
 - 2.2.2. One or more [REDACTED] encounter the incident 5
 - 2.2.3. All the [REDACTED] encounter the incident 5
 - 2.3 Communication with the [REDACTED] Provider outside the MCS..... 6
 - 2.4 Technical References..... 6

Notice	This document is part of the operational manual of ANIDOA and is governed by Change Control. Any change to this document shall follow the ANIDOA change control procedure. The content of this document might have evolved by the time you read or use this document. Please contact the PCR Change Control Administrator to check that this is the latest version before using this document.
---------------	--

1. Introduction

1.1. Purpose

The purpose of this procedure is to clarify the process of [REDACTED] incident management by describing the following actions:

- the steps that each [REDACTED] has to follow in case of a [REDACTED] incident during the Market Coupling Session (MCS);
- the process of investigating the incident by involving the IT department and the [REDACTED] Provider;
- the identification of the alternatives to resolve the incident;
- the implementation of the appropriate solution;
- the follow-up after the implementation of the solution.

The PMB Provider is UNICORN.

1.2. Governed / Regulated by

- Intra-Day Operational Agreement (IDOA)
- Intraday Auctions – Detailed design
- Intraday Auctions Implementation HLC
- Maintenance and Support Contract ([REDACTED] Provider)

1.3. Previous and next procedures

- All relevant ANIDOA procedures in case of an incident
- IDA_NEMO_OPE_01- IDA Coordinator Switch
- SIDC_JOINT_FAL_01 - Incident Management
- SIDC_JOINT_OTH_02 - Internal and External Communications
- Technical Infrastructure Documents

2. Procedure

2.1 Overview

The deliverables used in the Broker and Matcher (i.e. [REDACTED] application) gives the scope within which incidents have to be solved by the [REDACTED] provider.

The PMB provider will act upon request of:

- an [REDACTED]: in case only 1 [REDACTED] encounters the incident (identified as local incident) or
- the Incident Committee: in case it is not a local incident.

The [REDACTED] provider will act with the shortest delays to prevent or limit any impact on (the business continuity of) the [REDACTED] and prevent a Cancellation of Scheduled IDAs.

During operations, a request formulated by the [REDACTED] acting as [REDACTED] or [REDACTED] will be handled before any request from a [REDACTED].

Incident level	Description
Critical	An Incident that materially affects the use of the Market Coupling Systems and renders market coupling by means of the Market Coupling Systems impossible. No reasonable Workaround exists.
Major	An Incident, not being a Critical incident, that materially affects the use of one or more of the main functions of the Market Coupling Systems. If a Workaround is found for a Critical incident, it becomes a Major incident.
Minor	Any Incident other than a Critical or a Major Incident.

Request for a Critical or Major Incident solving may be formulated by a [REDACTED] to the PMB provider during 7 days per week, from 08:00 till 23:00 CET. Minor Incident solving may be requested at any time during normal working days and Czech Republic Office Hours (5/7) = 08:00 till 23:00 CET.

If a Critical Incident occurs the [REDACTED] provider shall give immediate, full attention to resolve the reported incident. This may involve (1) Source Code change and/or (2) any other type of solution.

(1) Source code change:

Corrective changes involving adaptation of the Source Code should be applied according to the contract. If the solution cannot be made in time for the Market Coupling Session of the same day, then it should be in place in time for the Market Coupling Session of the next day (i.e. on the next day at 8:00 a.m. at the latest).

(2) Other type of solution:

Any other type of solution (e.g. workarounds, configuration changes, restarts, database edits, etc.) shall be applied immediately by the [REDACTED] Provider and must aim at enabling the Market Coupling Session for the current day.

The support staff of [REDACTED] provider shall be provided with a remote connection, according to TeamViewer Procedure, to the production version of the Market Coupling Systems of [REDACTED] who encounters the incident (local) or the [REDACTED].

The [REDACTED] Provider will record all actions, including incoming and outgoing emails and calls, regarding the incident in the JIRA PCROPER project available at [REDACTED]

[It is recommended to submit incidents with prefix "\[REDACTED\]" in the title.](#)

Contact details

[REDACTED]
[REDACTED]
[REDACTED]

2.2 Communication with the [REDACTED] Provider during the MCS

When an [REDACTED] encounters an incident within the defined scope the [REDACTED] must be informed in order to trigger an Incident Committee, according to procedure - SIDC_JOINT_FAL_01 - Incident Management.

In parallel, the concerned [REDACTED] immediately requests the support of the IT department in resolving the incident and also to be able to set the remote access as soon as possible. The Incident Committee will investigate which [REDACTED] encounter the same incident. Depending on the outcome of the investigation, the steps to be performed are based on the following:

1. The [REDACTED] incident occurs only for the [REDACTED] – see 2.2.1;
2. The [REDACTED] incident occurs for one or more [REDACTED] (s) – see 2.2.2;
3. The [REDACTED] incident occurs for all [REDACTED] – see 2.2.3.

2.2.1. The [REDACTED] encounters the incident

If the [REDACTED] encounters the incident, the [REDACTED] will take over the [REDACTED] role, according to procedure - SIDC_JOINT_FAL_01-Incident Management.

If the [REDACTED] encounters the same incident, another [REDACTED] without [REDACTED] issues should take over the [REDACTED]

If the [REDACTED] switch is successful, all [REDACTED] must focus on continuing the Market Coupling Session in order not to lose time. The [REDACTED] reported the incident will use backup procedures for sending and receiving files to and from the [REDACTED]. Either in parallel or at the end of the Market Coupling Session, the concerned [REDACTED] takes local actions for contacting the [REDACTED] Provider in order to investigate and solve the issue.

2.2.2. One or more [REDACTED] encounter the incident

If one or more [REDACTED] encounter the incident, all [REDACTED] must focus on continuing the Market Coupling Session in order not to lose time. The [REDACTED] having reported the incident will use backup procedures for sending and receiving files to and from the IDA Coordinator.

Either in parallel or at the end of the Market Coupling Session, the concerned [REDACTED] take local actions for contacting the [REDACTED] in order to investigate and resolve the incident.

2.2.3. All the [REDACTED] encounter the incident

If all [REDACTED] experience the same incident, the [REDACTED] will immediately forward the Incident Committee invitation to the First Line Support [REDACTED] (SIDC_JOINT_OTH_02). The [REDACTED] Provider needs to join the IC as soon as possible, within 5 minutes. In case the [REDACTED] Provider does not respond within 5 minutes, the [REDACTED] must contact [REDACTED] Provider via phone.

As soon as the [REDACTED] Provider joins the Incident Committee, the [REDACTED] gives a brief description of the incident.

The [REDACTED] Provider starts investigating the incident giving the highest priority to the Coordinator's [REDACTED].

Remark: If the IC is too noisy for the [REDACTED] to follow the instructions given by the [REDACTED] provider, a bilateral call can be opened between the [REDACTED] and the [REDACTED] provider. In this case, the [REDACTED] will be involved in two different calls at the same time (the IC call and the bilateral call with the PMB Provider).

The IT department of the [REDACTED] provides [REDACTED] credentials (login and password) to the [REDACTED] Provider by email, in order to allow the remote connection to the [REDACTED] server. The [REDACTED] Provider proceeds with the remote connection and starts the on-site investigation. Once the cause of the incident is known, solutions should be discussed and in the IC decisions must be taken to start resolving the incident as fast as possible. Implementation of the solution must be coordinated by the [REDACTED]. Possible solutions:

- The [REDACTED] Provider provides a patch and sends it to the concerned [REDACTED] Operator(s) by email, using the contact list annexed to the procedure - SIDC_JOINT_OTH_02. The email will also include a clear set of instructions for installing the patch. All the concerned [REDACTED] follows the provided instructions accordingly. During the Incident Committee all [REDACTED] must authorize the implementation of the patch. The IT department of the concerned [REDACTED] installs the provided patch.
- The [REDACTED] Provider applies the correction directly in the [REDACTED] environment. Later, outside the Market Coupling Session, the [REDACTED] Provider sends the patch to the concerned [REDACTED] (s), according to section 2.3.

2.3 Communication with the [REDACTED] Provider outside the MCS

At the end of the Market Coupling Session where a [REDACTED] incident was encountered, an Incident Committee will be triggered in order to ensure the follow up of the incident.

The [REDACTED] Provider and the IT department of the concerned [REDACTED] (s) will be involved in the Incident Committee.

If not already done during the Market Coupling Session, the [REDACTED] Provider provides the corrective patch by email, using the contact list annexed to the procedure SIDC_JOINT_OTH_02. The email will also include a clear set of instructions for installing the patch. During the Incident Committee, all [REDACTED] must authorize the implementation of the patch. The patch installation will be performed by the IT departments as soon as possible, in order to ensure a proper [REDACTED] functioning for the following Market Coupling Session.

In the end, the [REDACTED] Provider will send a detailed incident report to all the [REDACTED], mentioning the cause of the incident, the solution applied and the steps of the implementation process.

2.4 Technical References

For technical details, see the following Technical Infrastructure Documents:

- [REDACTED] Procedure.

This is the same procedure as the one use in the Day Ahead. It is owned by all [REDACTED] parties but not shared on ProjectPlace.