NASDAQ OMX Nordic
Business Continuity Plan Description

October 10th, 2013

This document is valid for NASDAQ OMX Nordic, including the legal entities:
NASDAQ OMX Stockholm AB
NASDAQ OMX Copenhagen A/S
NASDAQ OMX Helsinki Ltd
NASDAQ OMX Iceland h.f.
NASDAQ OMX Tallinn AS
NASDAQ OMX Riga AS
AB NASDAQ OMX Vilnius
NASDAQ OMX Oslo ASA
NASDAQ OMX Clearing AB
Table of Contents

October 10th, 2013

1 Document Data .......................................................................................................................... 3
  1.1 Document Validity .................................................................................................................. 3
  1.2 Document Objectives ............................................................................................................. 5
  1.3 Audience .................................................................................................................................. 5
2 Introduction ................................................................................................................................. 6
3 Disaster Recovery ......................................................................................................................... 7
  3.1 System Redundancy and Fail-over ......................................................................................... 7
  3.2 Primary and Secondary Sites ................................................................................................. 7
  3.3 System Fail-over Procedures ................................................................................................. 7
    3.3.1 INET Nordics .................................................................................................................... 7
    3.3.2 Genium INET .................................................................................................................. 8
    3.3.3 Genium Market Info ....................................................................................................... 10
  3.4 Testing Site Functionality and Fail-over ............................................................................... 10
  3.5 Customer Fail-over Testing ................................................................................................. 10
    3.5.1 INET Nordics .................................................................................................................... 10
    3.5.2 Genium INET .................................................................................................................. 10
    3.5.3 Genium Market Info ....................................................................................................... 11
4 Contingency Plan ....................................................................................................................... 12
  4.1 Contingency Office ............................................................................................................... 12
  4.2 Mission Critical Activities .................................................................................................... 12
  4.3 Business Impact Analysis ..................................................................................................... 12
  4.4 Testing of the Contingency Office ....................................................................................... 12
  4.5 Communication Plan ............................................................................................................. 13
  4.6 Education and Training of Staff ............................................................................................ 13
5 System Load Testing .................................................................................................................. 14
  5.1 Pre-production Load Tests ................................................................................................. 14
  5.2 Load Testing .......................................................................................................................... 14
    5.2.1 INET Nordics .................................................................................................................... 14
    5.2.2 Genium INET .................................................................................................................. 14
    5.2.3 Genium Market Info ....................................................................................................... 14
  5.3 Customer Load Testing ......................................................................................................... 14
    5.3.1 INET Nordics .................................................................................................................... 14
    5.3.2 Genium INET .................................................................................................................. 14
    5.3.3 Genium Market Info ....................................................................................................... 14
6 System Load Monitoring .......................................................................................................... 16
  6.1 System Load monitoring ....................................................................................................... 16
1 Document Data

1.1 Document Validity

This document is valid for the legal entities:

- NASDAQ OMX Stockholm AB
- NASDAQ OMX Copenhagen A/S
- NASDAQ OMX Helsinki Ltd
- NASDAQ OMX Iceland h.f.
- NASDAQ OMX Tallinn AS
- NASDAQ OMX Riga AS
- AB NASDAQ OMX Vilnius
- NASDAQ OMX Oslo ASA
- NASDAQ OMX Clearing AB

The above listed entities use common trading systems, clearing system and related systems which enable efficient cross-border trading, cross membership, and one source for Nordic and Baltic market data. The operation of the systems is centralized to Stockholm, Sweden.

Henceforth in this document the following terms will be used:

- NASDAQ OMX, referring to the NASDAQ OMX Group.
- NASDAQ OMX Nordic, referring to all legal entities listed above (either each individually or all together).

The document is valid for the following legal entities:

<table>
<thead>
<tr>
<th>Legal entity</th>
<th>Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>NASDAQ OMX Stockholm AB</td>
<td>Stockholm Equities (including Oslo equities)</td>
</tr>
<tr>
<td></td>
<td>Stockholm Derivatives market (including derivatives on Swedish, Danish,</td>
</tr>
<tr>
<td></td>
<td>Finnish and Norwegian equities and indices)</td>
</tr>
<tr>
<td></td>
<td>Stockholm Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Copenhagen A/S</td>
<td>Copenhagen Equities</td>
</tr>
<tr>
<td></td>
<td>Copenhagen Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Helsinki Ltd</td>
<td>Helsinki Equities</td>
</tr>
<tr>
<td></td>
<td>Helsinki Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Iceland h.f.</td>
<td>Iceland Equities</td>
</tr>
<tr>
<td></td>
<td>Iceland Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Tallinn AS</td>
<td>Tallinn Equities</td>
</tr>
<tr>
<td></td>
<td>Tallinn Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Riga AS</td>
<td>Riga Equities</td>
</tr>
<tr>
<td></td>
<td>Riga Fixed Income</td>
</tr>
<tr>
<td>AB NASDAQ OMX Vilnius</td>
<td>Vilnius Equities</td>
</tr>
<tr>
<td></td>
<td>Vilnius Fixed Income</td>
</tr>
<tr>
<td>NASDAQ OMX Oslo ASA</td>
<td>Commodity Derivatives</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal entity</th>
<th>Clearing of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NASDAQ OMX Clearing AB</td>
<td>Stockholm Equity and Index derivatives (including derivatives on Swedish, Danish, Finnish and</td>
</tr>
</tbody>
</table>
### Norwegian equities and indices
- Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities)

### Commodity derivatives

---

This document applies to the operation of the following systems:

<table>
<thead>
<tr>
<th>System</th>
<th>Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>INET Nordics</td>
<td>Stockholm Equities (including Oslo equities)</td>
</tr>
<tr>
<td></td>
<td>Copenhagen Equities</td>
</tr>
<tr>
<td></td>
<td>Helsinki Equities</td>
</tr>
<tr>
<td></td>
<td>Iceland Equities</td>
</tr>
<tr>
<td></td>
<td>Iceland Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Tallinn Equities</td>
</tr>
<tr>
<td></td>
<td>Riga Equities</td>
</tr>
<tr>
<td></td>
<td>Vilnius Equities</td>
</tr>
<tr>
<td>Genium INET Trading</td>
<td>Stockholm Derivatives market (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices)</td>
</tr>
<tr>
<td></td>
<td>Stockholm Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Copenhagen Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Helsinki Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Tallinn Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Riga Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Vilnius Fixed Income</td>
</tr>
<tr>
<td></td>
<td>Commodity Derivatives</td>
</tr>
<tr>
<td>Genium Market Info</td>
<td>Market data from all above markets</td>
</tr>
<tr>
<td></td>
<td>Market data distribution system, for the market data product Genium Consolidated Feed (GCF). GCF disseminates consolidated real-time data from all NASDAQ OMX Stockholm source systems.</td>
</tr>
</tbody>
</table>

### Clearing of

<table>
<thead>
<tr>
<th>System</th>
<th>Clearing of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genium INET Clearing</td>
<td>Stockholm Equity and Indices derivatives (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices)</td>
</tr>
<tr>
<td></td>
<td>Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities)</td>
</tr>
<tr>
<td></td>
<td>Commodity derivatives</td>
</tr>
</tbody>
</table>
1.2 Document Objectives

This document describes the routines, organizations and arrangements that apply for maintaining the operation of NASDAQ OMX Nordic’s trading, clearing and other relevant systems in the event of an emergency. It covers how NASDAQ OMX Nordic organizes to handle emergencies, how the Business Continuity Plan is applied, and what features the Disaster Recovery sites offers. Furthermore, load testing and fail-over functionality are described. In addition, it describes the testing performed to maintain the arrangements above.

The purpose of the document is to provide information for audits or queries from external organizations.

1.3 Audience

The intended audience for this document includes external regulatory or supervisory parties, and participants.
2 Introduction

It is of utmost importance for NASDAQ OMX Nordic to provide solid and robust systems and procedures for the operation of the markets; including trading, clearing and other relevant systems. Any system disturbance or emergency must be addressed and resolved within the shortest time possible.

As a consequence, NASDAQ OMX Nordic has made extensive efforts and spent significant resources on dedicated organizations, routines and system solutions to minimize the impact of system disturbances or emergencies.
3 Disaster Recovery

The Disaster Recovery Plan (DRP) is part of the NASDAQ OMX Nordic Business Continuity Plan (BCP). The aim of the Disaster Recovery Plan is to outline the process and procedures put in place by NASDAQ OMX Nordic to ensure recovery and continuation of infrastructure critical to ensure that the business critical functions can be performed. The DRP focuses on the technology that supports business critical functions.

3.1 System Redundancy and Fail-over

NASDAQ OMX Nordic’s trading and clearing systems are designed to provide redundancy and fail-over functionality. The fail-over solution depends on the type of system and component involved. This is described in the following chapters (see 3.2 - 3.5).

3.2 Primary and Secondary Sites

NASDAQ OMX Nordic distributes its production systems on two separate sites with independent infrastructure, including their own power supply in order to ensure protection from power grid blackouts. The primary site is located in the Stockholm area, approx. 20 km from the secondary site. The secondary site acts as standby site, where systems and processes can be promoted to run as primary. From a connectivity standpoint the sites are equal. Customers are able to connect to either/both the primary or secondary site, thus being able to reduce their risk and lessen the impact of a system disturbance affecting one site. Both locations have a high security level both in terms of physical protection from fire or water etc., as well as any unauthorized access or other external threats.

3.3 System Fail-over Procedures

In the event of a serious system disturbance, making the primary site unable to continue operating, system operation will need to fail-over to the secondary site. The fail-over procedure differs between systems; it is mostly manual for INET and Genium INET, but automatic for Genium Market Info. The manual fail-over takes between 5 and 30 minutes to complete, depending on the type of failure and which system is affected. Fail-over functionality is divided into fail-over of back-end systems or components thereof, and fail-over of customer connections. Again, the behavior is different depending on which system and which protocols/API that are affected. Below is a concise description of the failover functionality per system and protocol/API.

3.3.1 INET Nordics

The INET Nordic central system components run on the primary site. The central systems on the secondary site are in hot standby mode. The FIX, OUCH and ITCH protocol connectors are active and available on both sites. OUCH and ITCH allow concurrent logons to primary and secondary site, and FIX allows logon to either primary or to secondary port at a time.

A fail-over of the INET Nordic central system is a manual process and will take approx. 30 min to complete.
3.3.1.1 FIX
The FIX protocol offers one FIX account use of ports on the primary or on the secondary site one at a time. FIX solution is hot-hot, meaning that FIX ports on both sites are on a listening state, and an instant failover with synchronized sequencing between primary and secondary site is available at any time. Failover is a client initiated process, and a logon made toward the secondary port will force a logoff if there is a client connected to the primary port (or vice versa). Customers are advised to use the ports on the primary site for the lowest latency.

In the event of a primary site failure, the FIX ports on the secondary site will not be possible to use until the routing engine is running in primary mode on the secondary site.

3.3.1.2 OUCH
The OUCH protocol offers one OUCH account concurrent use of ports on the primary and secondary site. Both OUCH ports will accept orders and cancel requests, and outbound messages will be sent on each port. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the OUCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

3.3.1.3 ITCH
The ITCH protocol offers one ITCH account concurrent use of ports on the primary and secondary site. Market data messaging can be received on both ITCH ports. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the ITCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

3.3.1.4 Co-Location services
Co-location customers normally have both the primary and the secondary ports located on the primary site, and are therefore unable to participate in a failover to the secondary site. These customers have the possibility to arrange their own connectivity to the secondary site or to co-locate at the secondary site.

In the event of a primary site failure, the customer would need to have connectivity and another set of FIX, OUCH and ITCH ports on the secondary site. If so, the FIX, OUCH and ITCH ports on the secondary site will not be possible to use until the routing and/or matching engine are running in primary mode on the secondary site.

3.3.2 Genium INET
The Genium INET central system components run on the primary site. The central systems on the secondary site are in hot standby mode. The OMnet Gateways are active and available on both sites.

A fail-over of the Genium INET central system is a manual process and will take approx. 30 min to complete.
3.3.2.1 OMnet
OMnet Gateways offers redundancy in two layers. The customers connect to single IP and port on a load balancer, which distributes the connection to one out of several physical OMnet Gateway behind it.

An individual OMnet Gateway failure will lead to loss of service for the customers connected to it. When the customer reconnects, the load balancer will direct the connection to another OMnet Gateway.

A failure of the connection between the OMnet Gateway and the transaction router that connects to the central system will cause a failover to another transaction router. The failover is automatic.

In the event of a primary site failure, customers will connect to the secondary site.

3.3.2.2 FIX
FIX fail-over is available in two phases, 1) between FIX gateways on the primary site, and 2) if the primary site is unavailable, to the secondary site:

The FIX gateways on the primary site are configured in pairs. Both FIX gateways in a pair are hosting primary connections. The corresponding secondary port is configured on the other FIX gateway. Customers are only able to connect to the primary port. In the event of a FIX gateway failure, the secondary ports will be enabled for connection. The FIX sequence numbers are shared between the FIX gateways, enabling a customer to continue on the secondary connection. The failover process is manual.

In the event of a primary site failure, the FIX gateways on the secondary site will be enabled for customer connections. Customers would need to connect to their primary port on the secondary site. The FIX gateways are in cold standby, meaning that sequence numbers from the primary site are not known. The FIX sessions are created as new sessions and customers need to reset the sequence numbers to 1. Again, the fail-over is manual process. There are no secondary FIX gateways on the secondary site.

3.3.2.3 ITCH
The ITCH protocol offers one ITCH account concurrent use of ports on the primary and secondary site. Market data messaging can be received on both ITCH ports. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the ITCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

3.3.2.4 Co-Location services
Co-location customers normally have both the primary and the secondary ports located on the primary site, and are therefore unable to participate in a failover to the secondary site. These customers have the possibility to arrange their own connectivity to the secondary site or to co-locate at the secondary site.

In the event of a primary site failure the customer would need to have connectivity to, or to be co-located on the secondary site. If so, the OMnet sessions, the FIX ports and the ITCH feeds on the secondary site will not be possible to use until the routing and/or matching engine are running in primary mode on the secondary site.
3.3.3 Genium Market Info
Genium Market Info (GMI) offers concurrent connections to receive the Genium Consolidated Feed. The Genium Market Info central system runs as a primary instance on the primary site, with a secondary instance on the secondary site. Data is replicated real time to the secondary instance, making the Genium Consolidated Feed available to customers connecting to either site.

INET, Genium INET and ICS are the main sources of raw market data to Genium Market Info. The services on the Genium Market Info central system are separated per source, enabling backend failover on a per source basis. As an example, INET and ICS could be sources for the Genium Market Info central system on one site, while Genium INET could have failed over to the other site. Irrespectively, the Genium Market Info system and hence the Genium Consolidated Feed will be available on both sites.

3.3.3.1 TIP
Genium Market Info offers concurrent connections to receive the Genium Consolidated Feed through the TIP protocol.

3.4 Testing Site Functionality and Fail-over
As a baseline, the current exchange and clearing systems have undergone thorough fail-over tests as part of the pre-production integration tests.

To exercise procedures and safeguard against possible errors in configuration, a full primary site failover test is performed on a yearly basis.

Central system component failover tests are performed as part of the required testing in conjunction with a major software release. Major releases are typically done on a yearly basis.

3.5 Customer Fail-over Testing
Fail-over functionality is available for all protocols/API. As mentioned in 3.2 and 3.3, customers can connect to either or both of the primary and secondary sites. It is important that customers can verify that their applications and their failover arrangements work as expected. To what extent this can be done in the production system depends on the type of system they connect to.

Customers are recommended to implement fail-over capacity in their applications. Certification of application fail-over capacity is offered but it’s not a mandatory requirement.

3.5.1 INET Nordics
Customers are advised to test fail-over procedures in the INET Nordic test system (OTF). System generated fail-over events are performed according to a weekly schedule. For the current fail-over setup please check schedule on the member extranet.

3.5.2 Genium INET
Genium INET central system failover tests for customers are performed as part of the required testing in conjunction with a major software release. Major releases are typically done on a yearly basis.
Customer failover testing can be performed and verified by the customers by dropping the connection to the primary site. If a customer should wish to simulate a fail-over without their own intervention, they can contact NASDAQ OMX Nordic business operations located in Stockholm for a forced shutdown of the chosen connection.

3.5.3 Genium Market Info

Genium Market Info offers concurrent connections to receive the Genium Consolidated Feed. Customers are recommended to connect to both sites in order to not lose any data. Fail-over can be tested and verified by customers by shutting down their own primary connections and switch to receiving data from the secondary connection, or in case of only! connecting to the primary, reconnect to the secondary site. If a customer should wish to simulate a fail-over without their own intervention, they can contact NASDAQ OMX Nordic business operations located in Stockholm for a forced shutdown of the chosen connection.
4 Contingency Plan

The Contingency Plan, which is part of the NASDAQ OMX Nordic Business Continuity Plan documentation (BCP), describes the objectives and procedures for how to keep business critical functions operating in a contingency mode in the event of an incident that cannot be managed by retaining full continuity and, if occurring, can threaten the company or its business operations. This includes procedures for relocation to the Contingency Office.

The complete Contingency Plan consists of a number of detailed documents and procedures describing:

- All mission critical activities
- Business impact analysis
- Internal and external communication plans
- Training and education plans
- Contingency Office test plans

This chapter will summarize these procedures in order to provide a high level understanding of the processes and controls put in place in order to ensure that business critical functions will be available to customers, suppliers and regulators in the event a relocation to the Contingency Office is needed.

4.1 Contingency Office

In case of an emergency situation resulting in evacuation of the NASDAQ OMX offices in Stockholm, the business operation will relocate to the Contingency Office. The office facilities and equipment is configured for maintaining the business operations with limited personnel. In an emergency situation additional operational personnel can log in and work from their homes or other location via their laptops and VPN connections.

4.2 Mission Critical Activities

A thorough analysis has been performed to identify a number of mission critical activities such as, but not limited to; trade support, order management, settlement management and exercise. For each activity the maximal acceptable outage time has been decided and deadlines and fixed delivery schedules have been determined.

To ensure that all activities can be performed from the Contingency Office, all relevant business applications have been installed on a number of desktop computers. All activities, hardware and software are tested on a monthly basis (see 4.4)

4.3 Business Impact Analysis

For each mission critical activity, potential events or threats (internal and external) that can cause interruption or other failure are identified. In addition to establishing acceptable outage times for each activity, each risk event has a detailed response plan outlining how to recover and uphold the activity.

4.4 Testing of the Contingency Office
In case of an emergency situation resulting in evacuation of the NASDAQ OMX offices in Stockholm where the business operation take place, the business operation will relocate to the Contingency Office.

In order to ensure that mission critical activities can be performed from the Contingency Office, employees handling these activities visit the site and execute critical routines on a rotating basis every 2nd month. Checklist reports are produced after each visit, and any issues such as faulty hardware, software and services are reported.

### 4.5 Communication Plan

In order to ensure regular updates to both internal and external parties in the event of a disaster, a communication plan has been established. The plan is a framework for internal and external communication and although the contents will vary depending on the situation it normally includes:

- **Internal communication plans relating to:**
  - Line management
  - Relevant Crisis Management Team
  - Affected staff
  - Internal Support Functions

- **External communication plans relating to:**
  - Customers (including members, vendors and listed companies)
  - Contractors and suppliers
  - Media
  - Regulating authorities
  - Cooperative ventures
  - Industry specific organizations

### 4.6 Education and Training of Staff

In order to ensure that staff are fully educated and trained, a mandatory BCP training course is set up for all new hires. In addition to this the capabilities of employees, systems and processes are verified through the bi-monthly Contingency Office review and the regular exercises. Relevant line managers are responsible and held responsible for ensuring that such reviews and training exercises have been conducted.
5 System Load Testing

5.1 Pre-production Load Tests

As a baseline, the current exchange and clearing systems have undergone thorough load (performance and capacity) tests as part of the pre-production integration tests. The tests have been done on the actual hardware and software configuration that has later been launched as production systems.

Load tests are also executed due to architectural changes in the systems. To ensure that new hardware and network solutions comply with the requirements, benchmark tests are performed. These are typically done with an 18-24 month interval.

5.2 Load Testing

Load tests executed in production and/or internal test systems differ depending on the type of system.

5.2.1 INET Nordics

INET load tests are performed in the INET Nordic test system (OTF) as part of the non-functional acceptance testing of a software release. The internal test system is equivalent to production in terms of capacity and performance.

5.2.2 Genium INET

Genium INET load tests are performed in the internal test systems as part of the non-functional acceptance testing of a major software release. The internal test systems are equivalent to production in terms of capacity and performance. Major releases are typically done on twice yearly.

5.2.3 Genium Market Info

There are no Genium Market Info load tests performed in the production environment, since only live production data is disseminated.

Load tests are performed in the internal test system as part of the non-functional acceptance testing of a major software release.

5.3 Customer Load Testing

The load testing available differs depending on the type of system.

5.3.1 INET Nordics

Customers are advised to perform or participate in load tests in the INET Nordic test system (OTF). System generated background and peak load is applied according to a weekly schedule. Peak load is adjusted to reflect loads seen in production. For the current load test setup please check schedule on the customer extranet.

5.3.2 Genium INET

Genium INET performance and capacity tests may be performed as part of the customer testing (MWAT) in conjunction with a major software release. Whether external load tests are executed depends on the content of the major release or system configuration. That is, if there are changes that affect performance and capacity in such a way that customers will need to verify their applications.

5.3.3 Genium Market Info
There are no separate Genium Market Info load tests available. When a load tests is executed in a source system, the market data feed in the corresponding Genium Market Info test system can be verified.
6 System Load Monitoring

6.1 System Load monitoring

Systems are monitored in several aspects, among them capacity and performance. Both standard and in-house developed tools are used in order to detect increase in capacity utilization and load. Key Performance Indicators are extracted on a daily basis and sent to operational personnel for evaluation. This type of data is also stored and used to create graphs that show trends, which is included in the monthly system operational reports.