# Business Continuity & Outage Plan

This document is published for informational purposes pursuant to Article 48 MiFID II, Article 18(5) MiFID II, Articles 15–17 of Commission Delegated Regulation (EU) 2017/584 (RTS 7), and the ESMA Opinion on Market Outages (ESMA70-156-6458, May 2023). It does not constitute advice or a recommendation of any product or service.

## 1. Infrastructure resilience

Aquis Exchange runs on the Equinox matching engine, an atomic broadcast distributed system designed with resilience at every layer. The platform operates across 16 European markets covering 6,500+ securities, with all markets operating on a shared infrastructure that isolates failures at the instrument, market and venue level.

### Automatic failover

Each matching engine instance has a primary and a secondary node, synchronised in real time. If the primary fails — whether hardware, software or network — the system automatically shifts processing to the secondary without manual intervention. Order and trade data is preserved across a failover; reconciliation reports are generated automatically to identify any gaps. All business-critical connectivity links have a dedicated secondary, configured to take over automatically upon failure.

### Data centre architecture

| Role | Provider & Location | Description |
|---|---|---|
| **Production** | Equinix LD4, Slough | Primary site. Redundant power, cooling and network. All exchange operations in normal conditions. |
| **Disaster Recovery** | Interxion LN1, London | DR site, 25+ miles from LD4. Continuously synchronised. Activated on failover decision; active for the remainder of the trading day. Physical access available within ~15 minutes. |
| **Data & Records** | AWS (cloud) | Market data, reference data and operational records. Built-in geographic redundancy; accessible independently of either data centre. |

### Continuous monitoring

The Operations and Infrastructure teams monitor the exchange platform, market data feeds, member connectivity and both data centres in real time throughout market hours. Monitoring covers infrastructure health, application status, message throughput and connectivity across all member sessions. Any degradation is detected and escalated immediately, triggering the incident management process described in Section 3.

## 2. Critical incident management

A **Critical Incident** is defined as any event that has halted the market entirely, or that has significantly impeded a material number of members from trading — due to a matching engine failure, market data dissemination issue, connectivity disruption or failure of market management tools. When a Critical Incident is declared, a dedicated response organisation is activated with shortened decision-making processes and direct management involvement.

### Priorities during a critical incident

1. Keep markets open for as long as they are operating in a fair and orderly manner.
2. Restore service as quickly and safely as possible, ensuring consistency between order and trade records at all times.
3. Communicate appropriately and in a timely manner to members, participants and the public.
4. Conduct a post-incident review and take corrective action to prevent recurrence.

### Decisions that may be taken during an outage

The CEO (or delegated authority: **COO** → **Head of Regulation** → **Head of Surveillance**) may take any of the following actions to protect market participants and maintain fair and orderly markets. At least one of these individuals is contactable at all times during market hours.

- Halt or suspend trading at market, instrument or venue level
- Cancel outstanding orders or bust trades executed under improper market conditions
- Suspend a member from trading
- Adjust market timetables, including delaying or cancelling trading phases
- Postpone or cancel the closing auction and use an alternative methodology to publish official closing prices
- Activate the disaster recovery site (LN1) to ensure business continuity

## 3. Communication during an outage

The outage plan is activated immediately upon any disruption — regardless of scale. All notices are published on the Aquis public website (**aquis.eu/status**) and distributed via the member notification service.

1. **Initial notice —** issued as soon as the outage is confirmed. Includes nature of the disruption, current market status and expected time of next update.
2. **Updates every 30 minutes —** throughout the incident, even where there is no material change to report.
3. **Resumption notice —** published at least 15 minutes before the pre-opening phase. Confirms the reopening timetable and allows members to update their orders before continuous trading resumes.

### Post-incident

Following every serious incident, Aquis conducts an internal root-cause review and identifies corrective actions. Significant system disruptions are reported to the FCA and relevant EU NCAs in accordance with Articles 31(2) and 54(2) of MiFID II. Any findings that require plan amendments are implemented before the next trading day where possible.

## 4. DR testing programme

Aquis conducts an annual DR testing programme, typically in Q4, comprising three planned weekend sessions as well as impromptu tests throughout the year. The programme covers both scheduled failover tests and unannounced tests designed to validate real incident readiness.

- **Internal DR weekend —** Infrastructure and Operations teams validate full failover to LN1 in a production-like environment, including platform hardware/network failure scenarios and office BCP procedures.
- **Member DR weekend —** members connect and trade on the LN1 environment, with connectivity, order entry, market data and drop copy validated end-to-end.

All test results are documented and submitted to senior management and the Board. Any significant failures must be rectified and re-tested within six months. The outage plan itself is reviewed at least every two years, in addition to the annual BCP review. Dates and joining instructions for member DR weekends are distributed via the member notification service.