

## **Business Continuity Disclosure**

### ***Plan Overview***

Neuberger Berman's Business Continuity Plan (the "Plan") has been developed to respond to a significant business disruption rendering any Neuberger Berman location inaccessible. Since the timing and impact of disasters and disruptions are unpredictable, the Plan allows for flexibility in responding to actual events as they occur. The Plan is designed to permit the firm to resume operations as quickly as possible, given the scope and severity of the business disruption.

Neuberger Berman has established a set of operating principles that govern how the Plan is enacted. The Plan's strategy for continuing business is to first ensure the safety and security of all employees and property. The Plan further addresses: data back-up and recovery for all mission-critical systems; financial and operational assessments to determine impact caused by the disruption event; alternative communications with customers, employees and regulators; alternate physical location of employees; critical supplier, bank and counter-party impact; protection of the firm's books and records in support of client, financial and regulatory reporting; and continued prompt access by clients to funds and securities. These principles are derived from an industry-wide set of best practices adapted to our firm's unique procedures, technologies, and markets.

### ***Incident Management***

The Incident Management Plan is maintained by the Business Continuity Management. The Incident Management Team has a specific set of roles and responsibilities that must be performed during an incident, including but not limited to incident assessment, recovery coordination, business strategy, technology recovery, logistics and communications. The team is activated from first response and function until business resumption.

### ***Alternative Employee Communications***

Communications with employees during a disaster will be accomplished via several methods:

Neuberger Berman has established an employee hotline for its US and European-based operations, where employees can hear recorded messages with information on office closures, relocation, and other pertinent data. This number has been printed on the back of all employee identification cards. Neuberger Berman also employs an automated notification tool to send recorded messages to all employees at home, work, and mobile phones. The tool is a third-party product and is hosted out-of-region, with an additional out-of-region backup facility.

The corporate intranet can be used to post messages to all employees on incident status and instructions for recovery. The corporate intranet is a highly-available web service that is housed in dual data centers.

### ***Alternative Locations***

Neuberger maintains a contract with a third-party vendor to supply physical recovery space for all critical Neuberger business functions that are performed in New York and throughout the United States, London, UK and throughout Europe . These contracts calls for work stations with desktop computers, phones, and network connectivity. Critical phone numbers will be re-routed to the recovery site.

### ***Technology, Data Recovery***

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, clearance, settlement, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities. Neuberger stores both physical and electronic copies of its data with third party agencies. Neuberger is currently dependent on multiple data centers in the United States. This design makes Neuberger's data highly available and resilient. "Mission critical systems" have their data replicated between data centers in real-time. This will allow Neuberger to failover and continue processing in the event of a datacenter disaster.

### ***Remote Access***

Remote Access is available whenever employees are away from the office. The NB Remote Access solution provides secure access to the user's applications and desktop from any internet connection. Multi-factor authentication (SecurID token) is utilized to control access and SSL is used to encrypt the user's session between their remote location and the corporate network. Remote access is tested on a regular basis to ensure that employees are familiar with how to use the system.

### ***Critical Business Constituents, Banks, and Counterparties***

Through its business continuity plan, Neuberger expects that it will maintain connectivity with all of its critical counterparties. However, in the event of a regional or wide-scale outage, Neuberger's ability to transact business with any critical bank or counterparty is dependent upon that organization's ability to perform its own recovery in a timely and effective way.

### ***Testing Procedures and Frequency***

Business Continuity and Disaster Recovery Tests are conducted at least annually. Tests include representatives from technology, critical business units, Internal Audit, and the Business Continuity team.

### ***Contacting Us***

In the event of a significant disruption, clients should refer to the Neuberger web site ([www.nb.com](http://www.nb.com)) or call one of the main Neuberger phone number listed below for information.

Americas:	212.476.9000
Asia:	81 3 5218 1930
Europe:	44 20 3214 9000

If you have questions about our business continuity planning program, you can contact your client services representative.