STANDARD &POOR'S

55 Water Street, 45th Floor
New York, NY 10041
Phn: 212.438.4589
Email: maria_mcisaac@sandp.com

Business Continuity and Disaster Recovery Planning Statement

The McGraw-Hill Companies' policy requires the development of Business Continuity plans. Standard and Poor's has adopted plans for Business Continuity Management (BCM), including Site Emergency Response (ER), Business Impact Analysis, Business Continuity Planning (BC), Contingency Planning, and Restoration Planning. Responsibility for BCM lies with Standard and Poor's CFO. BCM is administered by a BC coordinator and an ER coordinator, and overseen by a BCM Enterprise Risk Management subcommittee (ERM). The ERM subcommittee reports to the Standard & Poor's Enterprise Risk Management Committee, made up of members of the Standard & Poor's Executive Committee.

Standard & Poor's has developed internal policies and assigned responsibilities around the creation and maintenance of Business Continuity Plans (BCP). Standard & Poor's will continue to use reasonable efforts to review its BCPs consistent with industry practice. However, notwithstanding any statement in this Business Continuity and Disaster Recovery Planning Statement to the contrary, Standard & Poor's makes no express or implied representations, warranties or guarantees of the effectiveness or results of its BCPs.

S&P maintains BCPs consisting of Business Recovery Plans (BR), Disaster Recovery (DR), and Emergency Response Plans (ERP). Taken together, these plans address employee health and safety while at work, potential disruptions from the unanticipated loss of services or infrastructure, and management of resources for the resumption of business operations in the face of an emergency or disaster.

The BR Plan reflects a business impact analysis of the service level requirements for recovery, the clustering of business processes for optimal recovery, and recovery steps for each business process. These plans are produced and maintained in the global recovery information database (Strohl Systems LDRPS) accessible via the internet with appropriate authentication permitting access in the event of an incident. LRDPS is hosted at Strohl's headquarters in King of Prussia, PA, with full backup and disaster recovery.

BR plans also include instructions for mobilizing staff in the case of an emergency. In general, priority is given to processes that deliver products and services directly to S&P's customers and processes that provide customers with contracted deliverables at specific times. The target for recovering market-sensitive and/or mission critical processes is within 0-4 hours of the identification of a need to recover. The target for recovering the

balance of the business processes (non-market sensitive and non-business critical processes) is 4 to 48+ hours.

S&P's two data centers serve as backup for each other. They are staffed twenty-four hours a day, seven days a week and are equipped with redundancy and contingency features. The data centers are located approximately 50 miles apart, with one located in Standard & Poor's headquarters in New York City, and the other in a facility owned and operated by The McGraw-Hill Companies in Hightstown, New Jersey. S&P employs multiple Internet Service Providers and both data centers are equipped with dual entry paths for all major carriers and the ability to switch telecommunications between sites or to our domestic and overseas offices if necessary. Voice communications recovery planning takes advantage of support desks and distributed business lines that are prepared to pick up the message flow if a location loses that capability.

Both locations have uninterrupted power supplies (UPS) and generators as protection from drops, surges, or loss of voltage from the power utility. In the case of a utility outage longer than one minute in duration, the UPS will switch over to generator power. The generators can operate for approximately 35 hours before refueling. This time can potentially be increased through load shedding of non-mission critical equipment. Generators are tested weekly without invoking or moving the center over to that power grid. Annually, we perform full functionality tests of the UPS and generator, including infrared scanning for any potential heat loss on devices that may indicate failure.

There is approximately 800 tons of HVAC capacity built into the facilities. The on-site chiller plants with redundant pumps and compressors are maintained on a 24/7 basis

Physical access to the data centers is managed 24/7 by on-site security personnel and card-key access is required to enter the buildings and the data centers. Office space is also available or reserved in both data center locations to provide workspace for essential staff in the event of a disaster.

With regard to application systems recovery, each business unit makes use of the BR plan and works with its technology counterparts to assess the recovery requirements in the event of an interruption of processing. This information is used to establish service levels for application and data backup, failover and disaster recovery. Application architectures are implemented to support the service levels to meet or exceed recovery requirements. Implementations for market sensitive and mission critical systems often include data replication and load balancing to a mirrored site to protect information assets. Data for all business systems are backed up on a daily basis and the backups are stored at an alternative site managed by Iron Mountain, Boston MA. Backup, failover and recovery testing is scheduled on a periodic basis and new application systems' plans and budgets require recovery implementation and testing. A team dedicated to managing our application recovery plans keeps records of the entire application and database inventory, the service levels required for recovery, testing schedules and the status and budgets of recovery implementations for new application systems.

The Emergency Response/Incident Management Plan (ER/IMP) is updated on a quarterly basis and addresses the emergency response phase of the S&P Business Continuity Plan. It documents the emergency response procedures and personnel roles and responsibilities

in the event of a disaster. These plans are designed to be in alignment with Corporate policies, guidelines, and methodologies.

Pandemic Planning

Pandemic planning expands the S&P Business Continuity framework to address the threat of staff absenteeism for an extended period of time. In creating guidelines for use in the face of pandemic, S&P identifies critical business processes, business application and data center support needs, and addresses minimum staffing requirements across the firm. The S&P response plan employs a five-level pandemic response structure that integrates pandemic preparation with disaster recovery and emergency response plans. The pandemic response structure links to the World Heath Organization's Pandemic Alert Framework to calibrate the response of each business unit and the firm as a whole with the WHO pandemic alert level.

The McGraw-Hill Companies provides several solutions for employees to work from locations external to its global network. Business management determines which employees may work remotely and which solution is appropriate to the employee's need. For users who require simple access to e-mail, McGraw-Hill supports PDA access to its e-mail system via Good Technology's GoodLink product and via Research in Motion's Blackberry. There is adequate capacity in place to handle all McGraw-Hill employees. For users who require the ability to run business applications, McGraw-Hill provides two solutions for access to its network:

1. A VPN solution, which requires Nortel VPN client software. The VPN solution allows 12,500 concurrent connections across four global sites.
2. A Neoteris portal solution, which does not require client software, but which does require password access via RSA's SecurID authentication. The Neoteris portal allows for 3,000 concurrent connections across three global sites. Since the portal technology does not require client software, this allows approved users to access McGraw-Hill's network from any internet-connected computer (minimum browser version is required).

When connected via either of these solutions, the user can run business applications from a web browser if the application is web-enabled or through a Citrix session. McGraw-Hill's Citrix farm is currently load-balanced across five global sites and is built for full redundancy should any particular site fail.