CUSIP Global Services
Business Continuity Page

CUSIP Global Services Business Continuity Plan (BCP), calls for the relocation of CGS operations from New York City to its offsite facility in the event of an emergency. The following toll-free phone number has been set up to contact CGS at its BCP facility if relocation is deemed necessary:

1- 877- CUSIPDR
(1-877-287-4737)

Please retain this number for future reference.

During regular operations, you may continue to contact CGS at (212) 438-6500

Business Continuity and Disaster Recovery Planning Statement

The McGraw-Hill Companies' Corporate Policy Manual requires the development of Business Continuity plans for all segments of the Corporation. In keeping with Corporate policy, Standard and Poor’s has developed and maintains a Business Continuity Management (BCM) program in support of business recovery and continuity.

The S&P BCM program is managed day-to-day by a BCM Office that reports to S&P’s Senior Vice President, Finance and Administration through S&P’s Vice President of Enterprise Risk Management. The BCM program oversees business continuity planning worldwide. S&P’s business continuity plans include Emergency Response Plans, Business Impact Analyses, Pandemic Plans, Business Recovery Plans, and Disaster Recovery Plans.

Pandemic plans 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 Health 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.

Standard & Poor’s will continue to use reasonable efforts to review and maintain its plans in a manner consistent with industry practice. However, notwithstanding any statement in this Business Continuity and Disaster Recovery Planning
Statement, Standard & Poor’s makes no express or implied promises, representations, warranties or guarantees of the effectiveness or results of its business continuity plans or otherwise.

When addressing interruptions to technology, planning priority is generally 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 each market-sensitive or mission critical process 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 multiple data centers serve as backups to 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 in sufficiently diverse locations to mitigate a single event causing disruptions to the multiple data centers. The McGraw-Hill Companies employ multiple Internet Service Providers and the multiple data centers are equipped with dual entry paths for our selected data carriers as well as being engineered 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.

The data centers are designed to withstand power interruptions using uninterruptible power supplies (UPS) and generators as protection from drops, surges, or loss of voltage from the power utility. The generators can operate for approximately 35 hours once activated and before refueling. This time can potentially be increased through load shedding of non-mission critical equipment. Generators are tested monthly 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.

Sufficient cooling is available and all changes, both installing and removing equipment, reflect the impact to both power and cooling capacity on the data centers before the actual implementation.

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 maintains a Business Recovery plan developed with technology counterparts to assess 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.

Emergency Response Plans are location specific and address the emergency response phase of S&P Business Continuity Management planning. The plans document response procedures and personnel roles and responsibilities in the event of a disaster. These plans are designed to be in alignment with McGraw-Hill policies, guidelines, and methodologies.

The McGraw-Hill Companies provides several solutions for employees to work remotely 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 the ability to run business applications, McGraw-Hill provides two remote access connectivity solutions.
and using either of these solutions, the user can run business applications using virtual desktop technologies. McGraw-Hill’s virtual desktop solution is currently load-balanced across five global sites and is built for full redundancy should any particular site fail.

S&P’s plans are maintained in a global recovery information database (Strohl Systems’ LDRPS product) accessible via the internet with appropriate authentication permitting access in the event of an incident. LDRPS is hosted at Strohl’s headquarters in King of Prussia, PA, with full backup and disaster recovery.