Prudential is committed to providing uninterrupted service to our customers, protecting the assets they have entrusted with us and safeguarding our associates and resources.

Overview

The programs and plans we have put in place ensure the continuity of business and that we are there when our customers and business partners need us.
In support of our state of readiness, our Preparedness Strategy includes five areas:

1. Emergency Response,
2. Crisis Management,
3. Business Continuation Management,
4. Technology Disaster Recovery, and
5. Health Emergency Preparedness

The areas are built on programs, policies, standards, plans and training. We continually maintain and exercise our programs and plans according to the policies and standards. We have established objectives, metrics and reporting to provide a concise status of our readiness.

Our programs and plans leverage our diversity in personnel, locations and businesses as well as our global presence and robust/resilient infrastructure. These attributes ensure that we are prepared to address events of different sizes and scope that may threaten to disrupt business operations.

Emergency Response

Emergency Response to events is managed locally by a team consisting of facilities, security and medical personnel. Their role is to respond to the event in their location and minimizing impact to personnel/guests, assets and buildings. Their primary focus is safety and minimizing impact - Think of our facilities, security and medical personnel as our internal “first responders.”

In responding to emergencies, the facilities, security and medical personnel adhere to their established protocols and procedures. As part of their response, they will interact with the public sector first responders (police, fire and medical).

Crisis Management

Our Crisis Management Program includes the monitoring, response, communication, escalation and coordination activities required to effectively manage any event that may impact our services, associates or resources. Our escalation process and response protocols assist us in

handling any situation whether it requires our businesses continuation plans to be activated, is classified as a crisis or only requires monitoring. The following are six important elements within the Prudential Global Security Crisis Management Program:

1. Early warning mechanisms to identify signs and triggers of events that may escalate into a crisis.
2. Analysis and assessment of events to provide both tracking and trend reporting capabilities for domestic and international operations within Prudential.
3. Escalation and communication procedures to ensure that appropriate and consistent actions are taken.
4. Physical and virtual command centers to provide coordinated management of the event.
5. Crisis Management Plans to address and document contacts and responsibilities, as well as our response, communication, escalation activities.
6. Trained crisis management teams including the Enterprise Physical Security Crisis Management Team and Local Crisis Management Teams at locations with 50 or more employees in both US and non-US locations.

Whenever possible and appropriate, we utilize industry accepted tools and processes. We complement these tools and processes with internally developed systems to provide reliable solutions for preparedness. For example, we utilize an emergency notification system to readily communicate with our associates via various communication devices.

We partner with public sector entities and private sector peers for situational awareness and best practices. Our Crisis Management Program has focused on preparing for events ranging from active shooter and missing employees to civil unrest and severe weather. The Enterprise Physical Security Crisis Management Team (EPSMIT) receives information, makes decisions and coordinates activity across the company when a significant event occurs that could impact employees, facilities, operations, interests, brand or financials.

Business Continuation

Our commitment to providing continued service and safeguarding our customers and shareholders' interests means that we must ensure that we are prepared to continue critical business functions in the event of disruptions and outages of various types and scopes. This commitment and responsibility, down to the employee level, is documented in our standards and reinforced in our training programs. Where the Crisis Management Program focuses on our response to and management of events which may impact our operations, Business Continuation planning (BC) is a critical preparedness component to ensure our operations can continue or recover within expected timeframes. Business Continuation is the core of our Company's readiness state, and we believe we have a solid foundation in place as illustrated by the following attributes:

- A centralized function, Enterprise Business Continuation Management (EBCM) is accountable for developing and managing the Company's Business Continuation (BC) Program and monitoring its effectiveness.

- EBCM maintains standard operating procedures for BC planning and testing and ensures they are communicated globally.
- EBCM establishes and monitors metrics for BC planning deliverables, BC planning quality and completion of testing.
- Each business and corporate function has a BC Officer accountable for implementing the BC standards within their organization.
- Each BC Officer delivers an annual report to senior management and reviews their organization's program at the applicable business or corporate function Risk Committee.
- BC standards define required skills and training for BC Officers and BC Planners.
- Risk and control self-assessments are completed for the BC program of each business and corporate function.
- The BC Officers Council meets monthly to discuss risks, issues and program improvement areas.
- The BC Governance Council, which is comprised of senior leaders from each business and corporate function, meets quarterly to discuss BC operational risks, program initiatives and program changes.
- The Company's BC Program is reviewed annually with the Operational Risk Oversight Committee, Enterprise Risk Committee, and the Audit Committee of the Board.

Multiple BC Planners within each business and corporate function develop BC plans leveraging a standard process, which includes six steps.

1. Identify business processes and dependencies
2. Perform a business impact analysis
3. Validate dependency recovery objectives
4. Analyze business impact scenarios and develop recovery solutions
5. Develop and maintain BC plans
6. Test BC plans and solutions

Important elements of the BC Planning process include:

- Each business impact analysis and BC plan is approved by the applicable Department Head.
- Business and corporate function BC Officers oversee BC planning for their organizations.
- BC Officers conduct quality reviews of BC plans.
- Gaps between the recovery objectives of business processes and their dependencies are identified and addressed.
- BC plans are tested according to established frequencies.
- Employees receive annual awareness training on their BC plans
- BC planning addresses the following impact scenarios:
    - Unavailability or loss of people
    - Unavailability of dependent internal business processes
    - Unavailability of dependent internally hosted technology services
    - Unavailability or inaccessibility of primary work area, including city and regional events

- Unavailability of required third parties

Technology Disaster Recovery

Global Technology promotes a secure, efficient, and controlled data-processing environment across the enterprise. Prudential's Technology Organization manages robust data processing operations, keeping our technology operations safe and secure. Key highlights include:

- Tier 3 data centers have fully redundant power sources and utilize the modern fire protection solutions.
- Prudential has state-of-the-art, round-the-clock Operations and Cyber Security Control Centers that provide 24x7 intrusion detection, incident management, problem management, and centralized operations monitoring processes.
- Prudential technology operations employ the latest technology and processes for back-up/recovery and leverage multiple internal data centers providing recovery capabilities for mainframe, distributed, (i.e., includes storage, database and other components), and network infrastructure.
- All critical Prudential data is imaged between data centers and backed-up daily, then shipped to an off-site location as an additional failsafe.
- Prudential utilizes multiple call centers and remote access capabilities to allow business to continue across various locations.
- Prudential conducts disaster recovery tests on a regular basis, including four major data center test dates in the U.S. and full system recovery tests annually.
- The Technology Organization's BC Officer provides centralized technology BC planning, coordination and support. The Technology BC Officer serves as the liaison between Enterprise Business Continuation Management and Prudential's technology/infrastructure support teams.
- The Global Technology Organization manages the Enterprise IT infrastructure and Data Centers supporting business continuation and disaster recovery for Prudential's various lines of business.

Prudential's Information Security Office ensures that Prudential's information is kept safe and secure. Highlights of the Information Security program include:

- Enhanced controls to stay a step ahead of emerging threats including State-of-the-Art data protection and monitoring tools with 24x7 incident response capability.
- Ongoing virus and malware protection and email filtering.
- Robust vulnerability management and response readiness.
- Recurring network-level and application-level penetration testing.
- Ongoing phishing and awareness campaign with social engineering focus and recurring testing and real time user "coaching".
- Continual growth in correlation and intelligence capability to quickly defend against targeted malware.

- Detailed code review workflow within application development process to identify & remediate potential vulnerabilities during code development as well as routine scans of production code.
- The Information Security Office has focus on ransomware and Distributed Denial of Service accounts.
- Tabletop exercises around cyberthreats, and other technology security protocols are held with the technology and business leaders as well as annual testing of defensive controls to continue to raise awareness across the company.

Health Emergency Preparedness

Prudential's preparedness in the event a reduced workforce also addresses various health emergency scenarios. In 2005, Prudential formed a Pandemic Preparedness Planning Team that has matured into an Enterprise Health Emergency Team, chaired by Prudential's Chief Medical Officer. This corporate group has developed a comprehensive plan that addresses the needs of both our domestic and international businesses. This comprehensive plan has enabled us to analyze, train and test to address potential health threats including a new severe strain of the influenza virus, biological events or chemical hazards. The following are key elements of the plan:

- Monitoring of health concerns around the globe and early warning mechanisms
- Response protocols based on severity levels and phases
- Screening tools, social distancing procedures and cleaning/sanitizing protocols to limit exposure and spread
- A web-based health tool to assist associates with health-related questions and provide information to help them prepare in the event of a health emergency.
- Prudential's 24-hour Facilities Status extranet site and Facilities Status Hotline, which provides continuous updates to employees regarding Company information or building closures.
- Utilization of Crisis Management and Business Continuation programs and personnel to respond to a health emergency
- Prudential's Employee Assistance Program offers several support resources for employees and their family members during times of crisis

For more information on Prudential Financial Preparedness Strategy and individual programs, contact-

Prudential's Enterprise Business Continuation Management:
email Enterprise.BCM@prudential.com
OR
Prudential Global Security Command Center (staffed 24x7):
973-802-6675/email GSCC@prudential.com