

Continuity Plan Summary

Lincoln National Corporation (“LNC”) headquartered in Radnor, PA, is the parent corporation of, among others, The Lincoln National Life Insurance Company, First Penn-Pacific Life Insurance Company, and Lincoln Life & Annuity Company of New York. LNC’s subsidiaries have offices located in Atlanta, GA; Boston, MA; Charlotte, NC; Fort Wayne, IN; Greensboro, NC; Hartford, CT; Omaha, NE; Philadelphia, PA; Phoenix, AZ; Radnor, PA; Dover, NH; and Syracuse, NY. Lincoln Financial Advisors Corporation, Lincoln Financial Distributors, Inc., and Lincoln Financial Securities Corporation have business locations throughout the USA. Unless the context otherwise implies, as used herein LNC refers to LNC and its subsidiaries.

LNC is committed to safeguarding the interests of its clients and customers in the event of an emergency or significant business disruption (“SBD”). LNC’s broad business continuity strategy is designed to enable LNC to meet its existing obligations to its clients and customers in the event of an emergency or SBD by safeguarding employees and property, making a financial and operational assessment, recovering, and resuming operations, protecting LNC’s books and records, and allowing customers to conduct business.

Business Continuity Planning

LNC has a documented corporate policy requiring each Business Unit to develop a business continuity plan. In support of this policy, LNC’s Business Resilience area has the full-time responsibility of coordinating the development, testing and maintenance of all LNC Business Continuity Plans. Business Resilience determines and drives appropriate strategies for the development of a resilient business environment with formal systematic processes with auditable controls that enforces the corporate policy on continuity.

LNC’s Business Continuity Plans address advance preparations and actions to be taken in response to disruptions of various magnitudes. The Business Continuity Plans address the potential impact of varying risks of disruptions to LNC employees, equipment, computer and telecommunications systems, and office facilities. While it is impossible to anticipate every type of disruption that could affect LNC’s businesses, LNC takes an ‘all hazards’ approach to planning which encompasses reduction in workforce, loss of facility and loss of data.

Crisis Management

Local crisis management teams are in place in all LNC locations. These local crisis teams are charged with recording and managing any potential or actual crisis at the site from the time a situation occurs to the resolution of the incident and resumption of normal business operations.

Backup and Recovery

With the use of a co-located alternate Disaster Recovery data center solution LNC maintains back-up systems and power supplies that allow critical computer and telecommunications systems and facility functions to be maintained in the event of significant business disruption (“SBD”). The duration of the disruption will depend on the nature and extent of the emergency or SBD.

In the event of an SBD, where it is not possible to conduct business from one of LNC’s offices, the company will utilize work from home solutions as well as the use of alternate sites equipped with resources to support critical business operations.

LNC’s Business Continuity Plans are reviewed as necessary, and at least annually, to ensure they account for technology, business, operations, structure, or location.

Continuity Plan Summary

Critical Infrastructure and Application Testing

LNC's testing strategy incorporates the use of a Business Impact Analysis ("BIA") for developing enterprise-wide and Information Technology ("IT") Disaster Recovery ("DR") testing strategies. The strategy identifies key roles and responsibilities and establishes the minimum requirements for testing, including baseline requirements for frequency, objectives, and reporting test results. It also drives the requirements for creating and updating Disaster Recovery Plans and Validation Recovery documentation. Testing allows for the evaluation of the level of preparedness that exists in our environment and supports recommendations for resources and funding needed for compliance with applicable federal laws and regulations.

Lincoln completes scheduled annual testing focused on pre-defined parts of critical infrastructure. Tests are designed to establish and/or validate recovery time objectives. Additional tests are done periodically to recover individual applications based on criticality.

As an example, the scope of the tests may include:

- Evaluation of infrastructure (ex: computers, network, hardware) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Disaster Recovery tests are often included within these exercises.
- Operational readiness testing ("ORT") is used to conduct operational readiness (pre-release) of a product, service, or system and/or physical infrastructure (ex: building systems, generators, utilities). ORT may include checking the backup/restore facilities, IT disaster recovery procedures, maintenance tasks and periodic check of security vulnerabilities.
- Activities performed to evaluate a plan relative to specified objectives or measurement criteria.