FIRST HORIZON NATIONAL CORPORATION℠

firsthorizon.com

Business Continuity and Disaster Recovery Statement

At First Horizon Bank, First Horizon Advisors and FHN Financial (hereafter, collectively "First Horizon") we recognize that our customers rely on the availability of our systems and services. We also understand that the unexpected can, and occasionally does occur – from minor incidents to major outages.

To address these unplanned events, we have a business continuity and disaster recovery program that has successfully supported critical business activities during disruptions of normal business processes resulting from natural and man-made disasters, including, but not limited to, severe weather, fires, floods, earthquakes, pandemics, cyber and malware attacks.

How we are organized to respond:

Our Business Continuity (BC) and Disaster Recovery (DR) Program includes a dedicated team of certified business continuity and disaster recovery professionals.

- Our BC specialists work very closely with business units and the Enterprise Technology (ET) department to build and test comprehensive business continuity plans.
- Our DR specialists work directly with the responsible ET manager to develop comprehensive technology recovery plans.

The program is enterprise-wide with all business units required to develop, implement, test and maintain effective plans and recovery processes.

Managing Incidents

The mission of the Crisis Management Committee (CMC) is to ensure that the response to critical events impacting a member of the First Horizon family of companies is effectively assessed and managed. In addition, it prioritizes the safety and security of personnel, the functioning of core business operations, as well as provides timely communication to customers, business partners, regulators, shareholders, and the media. The CMC is comprised of the CEO and his direct reports, along with senior management and subject matter experts representing all key areas of the organization.

The Enterprise Technology division has also established an Incident Management team with formal processes on the notification, assessment, and management of all technology related incidents to ensure that outages are minimized and that technology applications and systems are available.

Emergency Response Teams for all critical locations have been designated to protect the safety of employees, customers, and visitors when a building evacuation and/or severe weather sheltering is necessary.

Business Continuity and Disaster Recovery: Eight Core Components

First Horizon Bank, First Horizon Advisors and FHN Financial operate under the Corporate Business Continuity Policy as approved by Executive Management and the Board of Directors. Leadership and direction of the program is governed by the Operational Risk Committee. Standards for business continuity and disaster recovery planning are outlined in the Business Continuity Planning Manual and include the following eight key components:

Business Impact Analysis Completion of the BIA allows for the recovery prioritization of all critical and time-sensitive processes.	• Assessment and prioritization of all business functions and processes, including their interdependencies. • Identification of the potential impact of business disruptions resulting from uncontrolled, non-specific events on all business processes. • Identification of the legal and regulatory requirements for all business processes. • Estimation of maximum acceptable downtime, as well as the acceptable level of losses, associated with all business processes. • Estimation of recovery time objectives (RTO), recovery point objectives (RPO), and recovery of the critical path.
Risk Assessment Business processes and the BIA assumptions are evaluated using various threat scenarios (loss of facility, loss of people, loss of technology, loss of vendor, and multiple loss of facility and people).	• Identify hazards and analyze threats based upon the impact to our company, customers, and the financial market we serve. • Prioritize potential business disruptions based upon their severity, which is determined by the probability of occurrence and impact on operations. • Perform a gap analysis that compares existing business continuity plan to the policies and their resulting impact.
Business Continuity Plan Comprehensive plan that details the strategies and procedures to recover, resume, and maintain all business processes.	• Overview with scope, objectives, assumptions and known issues. • Crisis management including emergency response procedures, succession plans, call lists, escalation plans, and recovery teams. • Teams and tasks outlining the roles and responsibilities for all team members, as well as tasks to be completed from the time of disruption through the point of recovery. • Critical locations including primary and alternate worksites, data centers, and off-site storage, along with the Crisis Management Command Center. • All business processes are evaluated with focus on critical business processes including non-standard or "work around" procedures. • Critical contacts including vendors, contractors, service providers, regulators, and key internal employee or department contacts. • Technology dependencies including hardware, software, operating systems, and recovery time objectives for restoring critical data and systems. • Vital records and off-site storage. • Equipment and supplies necessary to resume all business processes.
Technology Recovery Plan Comprehensive plan that details the strategies and procedures to recover, resume, and maintain all technology applications and operating systems.	• Overview with list of applications and operating systems covered. • Recovery team organization including key members from the business unit, technology department, and vendor. • Application specifications including RTO, RPO, required databases, scheduled job and transmissions, and other application dependencies. • Application connectivity diagram, firewall and communication requirements, and detailed step-by-step application recovery tasks. • Data verification procedures used to verify RPOs of all applications and operating systems. • Application specific services running on each server. • Application printing requirements, routing information, security requirements, and reliance on load balancing and clustering.

Relocation and Workspace Recovery Internal and external strategies utilized to aid in recovery efforts due to loss of or inability to access a facility.	Internal • Geographically dispersed hot-sites • Access to unoccupied workspace at existing company facilities. • Redeployment of existing workspace by displacing non-critical departments. • Utilization of existing work-from-home capabilities for designated employees. External • Access to vendor-supplied mobile workspace recovery units that can be deployed across our entire footprint within 48 hours. • Access to vendor supplied commercial and retail office space. • Access to vendor supplied emergency generators across our entire footprint. • Access to vendor supplied satellite connectivity to restore phone and Internet service

Testing
Risk monitoring and testing is necessary to ensure that the business continuity and disaster recovery planning process remains viable.
	• Development of an enterprise-wide testing program.
	• Assignment of roles and responsibilities for implementation of the testing program.
	• Completion of regularly-scheduled tests of the business continuity and technology recovery plans:
	  • Automated and manual call notification exercises, annually, at a minimum, for all departments.
	  • Tabletop exercises, in one to three year cycles, based upon plan criticality.
	  • Technology recovery exercises, including comprehensive annual data center recovery, and more frequent system-specific testing.
	  • Cyber attack exercises.
	  • Air gap exercises.
	  • Integrated recovery exercises including simultaneous recovery of technology and business processes.
	  • Pandemic / loss of people exercises.
	  • Crisis management exercises.
	  • Emergency management exercises including evacuation, earthquake and severe weather drills.
	  • Workspace recovery and work-from-home exercises.
	• Evaluation of the testing program and test results by senior management and the Board of Directors.
	• Revision of plans and testing program based upon lessons learned, changes in business operations, and test results.

Plan Validation and Management Certificate All business continuity plans are reviewed annually for quality and require a formal certification by responsible parties.	• Annual validation assesses each plan's overall quality, comprehensiveness, and compliance with FFIEC and FINRA guidelines, as well as procedures that should be implemented based on prioritized disruptions identified. • Annual plan certification requires attestation of recoverability by the business unit manager, technology manager, and business continuity relationship manager.
Internal and External Oversight Business continuity and disaster recovery program is in compliance with the requirements developed by the Federal Financial Institutions Examination Council (FFIEC).	• Annual report to senior management and to the Audit Committee of the Board of Directors of First Horizon. • Internal audits are completed annually along with continuous monitoring of the program and test plan. • Regular examinations completed by the Federal Reserve and the Tennessee Department of Financial Institutions.

Multi-Layer Data Protection and Recovery

First Horizon employs a multi-data center strategy in which critical data and systems are replicated to an alternate location ensuring accessibility in the event of a disaster. In addition, data retention and back-up procedures are in place, including tape back-up and off-site storage, offering an additional layer of data accessibility should the need arise.

First Horizon and its family of companies rely on geographically dispersed data centers to mitigate the risk of simultaneous loss of facilities. We currently leverage three geographically dispersed data centers. There are two primary data centers and two secondary or back-up data centers. In addition, some critical applications can be recovered to a tertiary data center.

Some systems and applications are hosted externally by third party service providers. The business continuity and disaster recovery plans for these vendors are reviewed annually to ensure the vendor has demonstrated the ability to recover applications and systems within the agreed timeframes to ensure the continuity of critical business processes.

Safeguarding our Technology Systems

First Horizon and its family of companies maintain a highly secure and redundant computing environment. The security models are audited by state and federal regulators consistent with our status as a state chartered bank. Our data security and recovery processes are reviewed by the Tennessee Department of Financial Institutions, and we remain in good standing.

First Horizon and its family of companies maintain detailed plans for conversion to back-up systems in the event of a disaster. Those documents contain confidential information about our security systems and are therefore not included as a part of this response.