usbank.com

U.S. Bancorp Enterprise Resiliency Program General Release Statement

The Enterprise Resiliency Program ("Program") establishes and supports the U.S. Bancorp ("Company") Business Continuity and Response Program. The Program is designed to protect customers, assets, and employees by evaluating the risks of significant adverse events; planning and validating response strategies; actively monitoring and reporting on the threat landscape and effectiveness of the control environment; and leading emergency response teams.

This Program ensures the Company and its affiliates meet the fiduciary responsibility to stakeholders and comply with regulatory requirements of the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Bank (FRB), the Financial Industry Regulatory Authority (FINRA), the Office of the Superintendent of Financial Institutions (OSFI), the Central Bank of Ireland (CBI) and the European Banking Authority (EBA). Additionally, Company has met all recovery criteria as prescribed by the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.

The U.S. Bancorp Board of Directors annually approves the U.S. Bancorp Enterprise Resiliency Policy. Program status and any significant issues are reported annually to the U.S. Bancorp Board of Directors and quarterly to the Managing Committee and Senior Executives.

Foundation of Risk Management

The Enterprise Resiliency Program is managed by a team of professionals specializing in resiliency and crisis management within the Company's Risk Management and Compliance division.

Risk Assessments

Risk assessments are foundational to the Program. The results of risk assessments drive the planning, exercising, and emergency response components of the program. The following risk assessments are performed:

- Business Impact Analysis ("BIA") measures the effects of resource loss and escalating losses over time to provide the basis for risk mitigation and business continuity planning. The BIA is completed annually or upon significant change for all critical business processes.
- Third-party Resiliency Assessment drives Third-party outage and recovery planning by evaluating the risks associated with mission critical third parties. The potential risks may include processes the Third-party performs or technology they manage or maintain operational support. Third-party Resiliency Assessments are completed annually or upon significant change to the relationship.
- Threat Vulnerability Assessment ("TVA") assesses the risk of major natural hazard events along with the impacts of those events on Company locations and the mission critical processes and technologies executed at those locations. The TVA is completed bi-annually or upon significant change.

Risk Mitigation Planning

The enterprise resiliency group maintains policy and standard that incorporates industry best practices for the operational resilience of critical business processes and technology. To achieve operational resilience, business process and technology owners, with oversight of the enterprise resiliency group, build and maintain response plans to address threats and risks identified by the assessment activities described above. The response plans are integrated into the overall Company Risk Management framework.

Business Continuity Response Plans

Company Business Continuity Plans are developed and maintained to address operational resilience and recovery strategies for events such as: pandemic/high employee absenteeism, natural and man-made hazard events, technology outages, cyber events, and other business disruptions.

In the event an office or operational facility is likely to become non-operational, an appropriate business continuity plan will be activated. The response strategy will vary based upon the nature of the disruption and work impacted.

Response strategies include:

- Transfer Work: Work is transferred out of the impacted area to another location that does the same business function or has been cross trained
- Relocate People within Business: Team members from the impacted location are relocated to another site
- Relocate to Regional Recovery Center: A location, other than the normal facility, is used to process data and conduct critical or necessary business functions
- Work from Home: Team members will work from home on bank secured devices

Company's business continuity response plans are reviewed and approved annually.

IT Resiliency Response Plans

Company's technology infrastructure is designed and implemented to ensure high availability and recoverability. Industry leading best practices and best-in-class technology components are utilized to operate a highly redundant, geographically dispersed network of data centers. All data is backed up to an out of region data center and all critical data is securely replicated to an out of region data center.

Company's IT Resiliency Plans are developed and maintained to address technology, infrastructure, application, and data recovery/ validation strategies in response to unplanned technology interruptions up to and including the loss of a data center.

IT Resiliency Plans are reviewed and approved annually.

Third-party Outage Response Plans

Third-party outage response plans are developed and maintained as a pre-planned response for mitigating and minimizing business impact when critical Third-party service(s) become impaired or unavailable because of an adverse event. Third-party outage response plans include but are not limited to the processes and procedures used for communicating, performing service continuity strategies, and for validating the resumption of services.

Third-party outage response plans are required to be reviewed and updated annually.

High Absenteeism/Pandemic Response Plans

The Company Pandemic Preparation and Response Plan is developed and maintained in partnership with senior leaders and other critical support departments to prepare for the possibility of a pandemic in the same way that we prepare for other events that could affect our employees, customers, and our communities. The plan was prepared in communication with public officials, pandemic planning experts, various state and local organizations, and other financial institutions and businesses. The plan augments procedures already in place as part of Company's existing program and outlines strategies to mitigate the impact of a pandemic upon the company, its employees, and customers.

Plan Validation

In alignment with regulatory requirements, Company policy, and industry best practices, resiliency plans are regularly exercised to demonstrate plan effectiveness and process/technology recoverability. Exercise scenarios include business continuity plan activation simulation; local, regional, national, and international crisis management and response team simulations; Company and Third-party joint exercises; and key/critical infrastructure/application technology resiliency.

Enterprise Resiliency Policy requires Business Continuity and Third-party outage response plans to be exercised annually. Technology resiliency plans for mission critical and key applications are exercised quarterly. Results from each exercise are documented and reviewed by the enterprise resiliency group. Any issues or plan discrepancies are documented along with remediation plans.

Crisis Management and Adverse Event Response

The enterprise resiliency group's Crisis Management Department manages and coordinates the enterprise response to adverse events that threaten to harm the organization, its stakeholders, employees, assets, or reputation. The enterprise response focuses on the safety of all employees, customers, and assets of the Company; minimizing disruption of service to customers; returning to a business-as-usual state as quickly as possible; and limiting any potential liability of the organization.

Employee Training and Awareness

Employee training and awareness is a critical component of the success of the program. The training and awareness consists of both formal and informal activities, including but not limited to: required biennial training courses; response team planning; participation in functional exercises of recovery plans; and localized evacuation procedure drills.

Audits/ Exams/ ISO Certification

Annual internal audits and periodic OCC/FRB exams are conducted on the company program. The enterprise resiliency program maintains an ISO 22301-Business Continuity Management certification.

Disclaimer

This document is subject to modification by U.S. Bancorp at any time.