Federated Hermes
Business Continuity Statement

Federated Hermes is committed to maintaining the operational integrity of critical business functions as well as the reduction and elimination of potential risks and vulnerabilities that could result from disruptions to firmwide operations caused by natural, technical, or human threats.

Corporate Business Continuity

Federated Hermes has established an Enterprise Business Continuity organization, which includes a Director of Enterprise Business Continuity who is charged with implementing and coordinating all business continuity activities.

Federated Hermes has an established global business continuity strategy which is supported by appropriate policies and procedures as well as an enterprise-wide business continuity organizational structure to ensure execution of the business continuity strategy.

The major objectives of Federated Hermes' Enterprise Business Continuity Program are to:

- Provide the framework for crisis management and business continuity planning
- Provide for the safety and welfare of employees and guests during a disruption
- Oversee the maintenance of contingency response plans and recovery strategies, firm-wide to ensure the continuity of vital client services during a disruptive event
- Ensure compliance with business continuity-related regulatory obligations and guidelines

Program Overview

Enterprise Business Continuity has a dedicated team of four that reports through the Chief Information Officer. Each business unit maintains a Business Continuity Liaison who, under the guidance of the Enterprise Business Continuity team, is responsible for updating their unit's continuity plan using a cloud-based continuity planning system. Plans are reviewed by the unit head at a minimum.

Each plan review cycle includes a thorough business impact analysis with a maximum allowable downtime for all processes. It also addresses the required information technology, staffing, invocation, and recovery procedures for the unit.

Federated Hermes employs multiple strategies for recovering critical staff and business processes, including remote access/work from home, shifting workload to alternate locations, or shifting work to a vendor. The firm employs a proactive, multi-layered approach to technology recovery that provides high availability for mission-critical systems with real-time redundancy and replication.

We have a comprehensive event response and communication program that enables the

firm to respond to disruptive events quickly. The firm utilizes an "off-prem" automated notification system to provide emergency messages to response teams and employees.

Technology

Federated Hermes maintains a state-of-the-art computing infrastructure designed for operational efficiency, high availability, security, and system redundancy. Our data centers are highly robust and operate to ensure that systems remain highly available, even during adverse conditions. We also leverage redundant cloud technologies. They are supported by redundant telecom and power from diverse paths, fire suppression, UPS, and backup power generation, all of which are tested on a regular basis.

In the unlikely event a data center should experience a catastrophic failure, the technology architecture can recover all critical information systems at the remaining data center within application-specified time frames.

Enterprise Business Continuity also works with all business units to identify critical applications in their business continuity plans. All business units are expected to develop alternate workarounds for the loss of all critical applications.

Testing

Exercises verify that the resources necessary for recovering critical business functions are available in the required time. Various types of continuity-related exercises are performed throughout the year. The frequency of testing is based on the criticality of the business unit or when significant organizational or technological changes warrant testing. Critical business units are required to test their recovery capabilities annually at a minimum. Recovery testing for critical information systems is conducted bi-annually.

Key Vendors

Federated Hermes' business continuity plans include connectivity to key vendors. Key vendors include, but are not limited to, market data providers, electronic trading networks, transfer agencies, fund accountants, and custodial banks.

Federated Hermes maintains a vendor risk program, which includes reviewing critical vendors' business continuity plans to ensure they are sufficient to provide continued service during a disruption of their own. This review may include participation in a vendor's disaster recovery tests, when appropriate.

Enterprise Business Continuity also works with all business units to identify critical vendors in their business continuity plans. All business units are expected to develop alternate workarounds for the loss of all critical vendors.

Federated Hermes' business continuity plans include procedures to provide necessary contact with clients and markets during an event.

As necessary, Federated Hermes may revise its business continuity program; the most current plan summary is posted on the Federated Hermes' website. Additional inquiries regarding Federated Hermes' business continuity program can be addressed to: CorporateBusinessContinuity@federatedhermes.com.