HIOP INDIA MANAGER IFSC PRIVATE LIMITED

DISASTER RECOVERY / BUSINESS CONTINUITY PLAN (DR/BCP)

Version	Date	Person Responsible
1	04-08-2025	Principal Officer

CIN: U66300GJ2023PTC146329
Regd Address: Unit no.B_118,Plot T1&T4Road 13,Block 11,SEZ,GIFT, Gift City, Gandhi Nagar, Gandhinagar, Gujarat, India
Email ID: HIOP.Compliance@hines.com
TEL + 91 124 480 2222

1. Hines Business Continuity / Disaster Recovery Plan Summary

Hines is committed to providing timely service to its clients, tenants, and investors around the globe. One of the areas in which we strive to excel is disaster readiness - to be prepared for scenarios which might challenge our ability to easily deliver the service levels we are accustomed to providing. We have a global response team in place including leaders in Administration, Operation, Engineering, Human Resources, IT, Accounting, Marketing and Communications, Risk Management, and Investor Relations. In addition, our critical systems are web-enabled and cloud-based. We maintain and update continuity plans regularly for all areas of the business to ensure proper resources are available to provide for operations during a crisis period, including reduced property staffing and working from home, as well as for the recovery and timely resumption of critical business operations. Crisis communications are handled through dedicated help lines and conference bridges as well as specially designated guidelines for posting information on the firm's intranet site. Additionally, Hines has a Crisis Response Team that works annually with the various lines of business and shared services organizations to ensure that the business continuity plan remains current.

2. Strategy

Corporate Office and Staff

Hines' U.S. corporate headquarters is located in Houston, Texas. The headquarters office serves as the primary site for our executive office, Corporate Communications, Human Resources, Finance and Accounting, Legal, Tax, Internal Audit, Compliance, Investment Management, Global Management Services (Property Management) and Engineering Services, Facilities Management, Multifamily, Client Strategy, Workplace as a Service), Sustainability, Hines Advisors/Core Fund, Fund Accounting Groups, Information Technology, Risk Management, Marketing and Communications, and other departments. . In the event of a disaster that would make the headquarters office unserviceable, staff will work remotely from dispersed locations, such as their private homes, hotels, third-party offices, or other locations.

Mission-Critical Departments

Hines recognizes that a disaster that would destroy any of its offices or computer facility locations would pose a significant operational risk. To mitigate this risk, Hines has policies and procedures in place that constitute a corporate business continuity program. The headquarters office serves as the primary location for our mission-critical departments, including Cash Management, Corporate Services, Capital Markets Internal Sales, Information Technology, Payroll, and Risk Management. There are documented and tested plans in place for each of these departments. Redundancies have been implemented and tested for these critical operational functions, including the ability to work remotely without any notice.

Hines Global Data Center Operations

All operations of the Hines Global Data Center are located at a cloud-based provider within the United States. Applications are protected by redundant servers whenever possible, and critical systems are hosted in separate physical locations within the cloud provider's infrastructure. Our Data Center Partner also maintains a secondary disaster recovery infrastructure in the same cloud provider, but in a geographically disparate location. The Partner maintains data backups as part of the cloud provider's operating strategy. Full backups are taken nightly, with incremental backups occurring during the day in order to meet the stringent Recovery Time Objectives (RTO). The cloud provider is responsible for ensuring optimal uptime and operating conditions for the hardware it hosts on behalf of Hines and its Technical Partner. The data center is equipped with multiple points of Internet circuit access for redundancy, as well as a fully-meshed private VPN network to all Hines building/office locations.

In the event of a disaster, the recovery plan will be activated. The Hines Disaster Recovery Organization consists of critical business and IT personnel and the Disaster Recovery Coordinator. The team's mission is to restore operations within the Recovery Time Objective ("RTO") for any impairment to global data center operations. For additional information such as Recovery Time Objectives, Fail-Safe Decision Points, etc. please refer to the separate detailed IT Disaster Recovery Plan.

Business continuity procedures are tested annually, in addition to semi-annually for some systems and quarterly for the JD Edwards ERP platform. Testing is spread throughout the year. Furthermore, IT-related continuity areas are reviewed annually in the Audit of all key IT controls and as part of the Firm's SOC 1 audit.

3. Business Scenario Preparedness

Office Locations

To ensure that Hines is ready to respond in a coordinated manner to natural disasters and emergencies, resources are available to all offices for creating a customized site-specific emergency response and contingency plan, which are tested periodically. If Hines loses the ability to perform business at one of the office locations, functions would be relocated to an alternative site (e.g., another location, home, hotel, third-party site) in an unaffected area. Each location has plans in place for this recovery and they are tested periodically. Recovery time objectives vary based on the criticality of each function. Larger offices also maintain backup Internet circuits for redundancy. Any onsite servers at a property location are backed up nightly using a cloud-based backup service and backup files are only accessible to a member of the Central IT Infrastructure Team. Any onsite server and network device must reside in a secure server room. Only people authorized as designated IT personnel are permitted access to a server room. Air temperature and humidity are controlled within acceptable limits to prevent damage to equipment. Any onsite server and network device must utilize a Uninterruptible Power Supply (UPS).

Additional support and tools (Hines Emergency Response Plan Guide) are provided to properties and regions by Hines Corporate Operations and Engineering Services and the Central Crisis Committee with members from Human Resources, Corporate Operations and Engineering Services, Information Technology, Risk Management, and Marketing and Communications**.**

Remote Data Center

If Hines loses the ability to perform business in its primary cloud-hosted location, Hines IT and its Technical Partner will fail over to its disaster recovery location. Plans are in place and are tested at least annually.

Pandemic Event

Hines has pandemic preparedness plans in place to continue business during a pandemic event. Our plan was designed by a team of employees from varying disciplines and public health experts with consult from International SOS and Corporate Medical Advisors.

This plan has two main components – a plan to prepare for and mitigate pandemic threats on Hines' employees and employee-occupied spaces, as well as a plan to prepare and mitigate pandemic threats on the spaces that we manage for our tenants, occupants, owners and other stakeholders.

This plan incorporates lessons learned from COVID-19 and other prior pandemics, as well as the latest expertise in this area to guide our response to pandemic threats. This preparedness plan provides guidance on when, how, and what type of preventive and mitigation measures we may implement, as well as how we can relax mitigation measures and return to operations in consultation with our stakeholders. It provides resources where we can find the latest epidemiologic and medical information to guide our response, as well as how we must balance the complexities of local, regional and national regulations along with our internal guidance.

Delegation of Authority Plan

In event of a disaster or emergency that results in the incapacitation of one of our key senior leaders including the Office of the CEO, we have developed a Delegation of Authority Plan that ensures able personnel with necessary skills and expertise can step into roles as needed and safeguard mission-critical operations. This Delegation of Authority Plan includes the full breadth of Hines' global firm. The plan is updated on an annual basis and maintained by our firm's legal department. Our legal team facilitates conversations with senior leaders to ensure the list is accurate and reflective of key needs and priorities. This enables us to be ready to activate an appropriate and timely response as soon as an incident arises.

Business Continuity Testing

The Hines business continuity program was tested when Houston suffered a direct hit by Hurricane Ike in 2008, Hurricane Harvey in 2017 and during the COVID-19 crisis. Critical systems including cash management, payroll and IT did not experience down-time or were restored immediately due to in-place redundancies and successful preparation. Further with the extended duration of distributed working (i.e. Work from Home, etc.) during the pandemic and ongoing as a new norm, many aspects previously categorized as 'business continuity aspects' are now considered normal daily operations.

Regulated Entities

Different regulated entities within the firm, including Hines Securities, Inc., HEREI, Hines Luxembourg Investment Management, and others have business continuity plans in accordance with relevant regulatory requirements.

4. Conclusion

Please be aware that, while we have detailed plans in place, we cannot guarantee that we will be successful in achieving recovery in the times noted above. For example, we may not be able to implement a plan during a disaster as quickly as we expect, or there may be disasters that we have been unable to anticipate and for which we have no plan. Additionally, if parts of our plan are dependent upon third parties, we will have no control over the success or failure of the third party to respond appropriately to the challenges posed at the time of the disaster.