DIAMOND HILL

INVESTED IN THE LONG RUN

Business Continuity Planning

Diamond Hill Capital Management, Inc. has developed and maintains a Business Continuity Plan (the "Plan") addressing intraday business disruptions as well as significant disruptions of a longer duration. The Plan is designed to protect client interests by providing a stable and reliable operating infrastructure to allow Diamond Hill to continue the management of client portfolios in the event of various business disruptions. The Plan includes an inventory of systems, back-up routines, alternate site information, remote access capabilities, communication protocols, and testing procedures.

Diamond Hill performs backup and recovery procedures utilizing a combination of three different methods: real-time replication with near-zero data loss; scheduled daily backups using replication software; and daily backups to external hard drives that are sent to a secure offsite location. The determination of which methods are used for backup and recovery is driven by system criticality. Notably, applications associated with trading, portfolio accounting, and other mission critical systems are replicated in real-time to a third-party data center that is audited in accordance with SSAE-19 SOC1 and SOC2, HIPAA, and PCI standards. Less critical applications are also replicated daily to the same data center. All critical workstations and servers are connected to an uninterruptable power supply (UPS) and a back-up generator for longer power disruptions. Server room environmental conditions are continuously monitored. Our business continuity data center is protected by an onsite redundant direct natural gas generator.

Disaster Recovery Testing

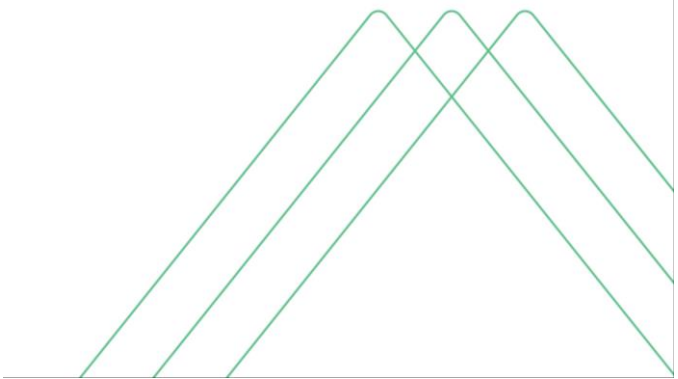
We routinely perform disaster recovery tests which are based upon two different test scenarios. Under scenario one, we assume that our permanent site and its network is intact; however, we are prohibited from entering the building or have made a decision to restrict office access. This scenario includes events such as a snow emergency, environmental hazard, or pandemic. Scenario two assumes that systems within the primary data center are not functional or the entire data center is no longer operational. For testing purposes, this scenario also considers the relocation of personnel to either the disaster recovery site or their homes. Triggering events include a cyber-security event, fire in the office space, or any scenario that would impact the company's technical infrastructure.

Test scenario one (access to the building is restricted/production data center intact) is tested throughout the year when staff members work from home and connect to the company infrastructure using Virtual Private Network (VPN) technology.

Test scenario two (access to the building is restricted / system malfunction or environmental impact) requires testing at our disaster recovery site and / or employee home locations. Diamond Hill performs scenario two disaster recovery tests on an annual basis. More frequent tests may be performed when major technology changes occur.

Commitment to Ongoing Testing

Diamond Hill maintains a strong commitment to routinely test mission-critical applications and keeps business continuity planning at the forefront of our resiliency initiatives. We make every effort to safeguard client data and as such, each test will be designed to verify that we can continue our business in the event of a business disruption while at the same time ensuring that client information is secure.



June 2023