

## **SYCAMORE SERVICES, INC.**

### **System Back-Up Disaster Recovery Plan & Specifications**

#### **Mission & Requirements**

Sycamore Services, Inc. having business critical data being produced from both daily business and administrative functions as well as from the storage of client related information requires a comprehensive backup and disaster recovery plan. The plan requirements are as follows:

- 1) On-site replication of data
- 2) Off-site replication of data
- 3) Compliance with regulations governing the storage of privacy sensitive information
- 4) The ability to recover business operations quickly in the event of a disaster
- 5) Space for Expansion at a rate of 20% per annum over 5 years

#### **Environment to Be Protected**

The main focus of this implementation is to protect the central storage of all server, client, and user data. End user's individual PCs are not to be included at this time.

The environment to be protected is entirely contained within a Software Defined Datacenter powered by VMWare. This consists of two ESXi host nodes and a block storage device (SAN) containing targets for all SDDC related Data Stores, containing Compute Instance VHDs, and targets for all Compute Instance related data drives. These drives include but are not limited to data drives for Provide / Accel, Accounting, and SQL.

#### **Technical Approach**

The BDR system uses a wedge type HDD driver agent which takes a block level snapshot of each compute instance and all its additional storage drives and stores this on the on-site BDR server as Virtual Hard Disk Drives. These block snapshots are then compressed, encrypted, and replicated daily to off-site cloud storage.

#### **Retention**

The system takes block level backups daily during the overnight hours. These are replicated daily to the cloud. 7 daily, 4 weekly, 12 monthly, and 1 yearly retention points are kept available locally. 1 daily, 1 weekly, and 1 monthly points are kept in the cloud.

#### **File Recovery**

Individual files may be quickly and easily recovered using a VHD file explorer to access any retention point VHD on the local BDR server. These files are stored in an encrypted format, so the decryption key is required for access.

#### **Disaster Recovery**

After backup, each compute instance backup is subjected to verification. Part of this verification process includes ensuring the compute instance backup will boot as a virtual machine using a

Hyper-Visor on the BDR server. These backups are then made available to run as virtual machines on the BDR server in the event of a disaster. The backups can also be run as virtual machines in the cloud in the event of a major disaster. This ensures business continuity within hours even in the event of a major disaster requiring physical relocation of employees.

### **Data Protection**

Block level backups are encrypted before they are transmitted to the BDR server. They are stored on the BDR server in encrypted format and they are transmitted to the cloud in encrypted format. The BDR system is Linux Based, not domain joined, and uses completely different passwords from all other IT resources. The BDR server also has no SMB or other file sharing services running on it. All this helps ensure that in the event of a Ransomware or other Malware or Virus infection it will not spread to the BDR server. Also, the use of block level VHDs ensures that an infection, even if it gets backed up, will not affect other restoration points associated with that server or any others.

### **Monitoring**

All aspects of Backup, Verification, and Replication are monitored 24/7 by our IT Service Provider, One Choice Technology's, Network Operations Center. Our BDR contract with them is turn-key in nature and the NOC automatically addresses all backup related issues as they come up. This ensures timely daily backups are maintained without administrative intervention or approvals required.

### **Paper Records Storage**

- 1) Corporate records, as applicable, will be maintained on-site in fireproof, locked files or off-site in a bank safe box. These files may include:
  - a. Corporate documents
  - b. Titles of real and personal property
  - c. Payroll and related records
  - d. Human resources employee files
  - e. Key financial records
- 2) Records excluding current and prior year activity will be stored off-site in accordance with the record retention schedule.
- 3) Department Directors identify critical forms, files, and other records that are stored off-site and readily accessible in the event of a disaster or an audit. This would only include those files and records that are unique to that department since most may be obtained from other Agency locations.

  
Approved

11-18-18  
Date