Innovative Business Software, Inc.

Backup Policy

Appropriate security measures are to be implemented for backups, which includes all necessary physical security controls, such as those related to the safety and security of the actual backup media – specifically – disks, taps, and any other medium containing backup data. This requires the use of computer rooms or their designated area (facility) that is secured and always monitored and whereby only authorized personnel have physical access to the backups. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls.

- Constructed in a manner allowing for the adequate protection of backup.
- Security alarms that are active during non-business hours, with alarm notification directly answered by a third-party security service or local police force.
- The use of cages, cabinets, or other designated, secured areas for securing backups.
- Access control mechanism consisting of traditional lock and key, and/or electronic access controls systems (ACS), such as badge reader and biometric recognition (i.e. iris, palm, fingerprint scanners/readers). Furthermore, all electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of 30 days.
- Adequate close-circuit monitoring, video surveillance as needed, both internally and externally, with all videos are kept for a minimum of 14 days for purposes of meeting security best practices and various regulatory requirements.
- Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission critical areas.
- Appropriate power protection device for ensuring a continued, balanced load of power to the facility for where the backup resides.

BACKUP STRATEGY

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is to be determined.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations – Opus (MAA) Data center	Frequency • Full backups of the VM environment are completed on a daily basis after midnight at 2:00AM EST and ran through the morning hours. Retention Period • Backups of the VM environment are stored for at least 14 days.

	Storage Location • Storage of VM backups are kept onsite in the OPUS datacenter in Manassas, VA Recovery Time • Backups can start restoring within minutes. Recovery time is dependent upon the size of the VM, the backup itself, or how far back the restoration or rollback is coming from.
IT Operations – Vazata (DAA) Data center	Frequency • Full backups of the VM environment are completed on a daily basis after 7:00PM CST and are ran through the morning hours. Retention Period • Backups of the VM environment are stored for at least 14 days. Storage Location • Storage of VM backups are kept onsite in the Vazata datacenter in Dallas, TX. Recovery Time • Backups can start restoring within minutes. Recovery time is dependent upon the size of the VM, the backup itself, or how far back the restoration or rollback is coming from.
IT operations - Hardware Receivers	• Physical hardware such as receivers, routers, firewalls, gateways, switches, or other equipment and their configurations are stored onsite within the Dallas datacenter on an external network device. In the event of a restore being required, configs can be pulled from the external network drive and reloaded into the piece of equipment needing restored. • In the event of an equipment failure (i.e. – Firewall), all physical equipment is redundant to avoid service interruptions, as well as to provide lead time to order and/or replace failed equipment.
Disaster Recovery	• Any need for a restore point (i.e. – a backup) to be loaded into the SBN Cloud environment must first be addressed to the CTO of the company stating why a restore point is needed, what/who it impacts, as well as written approval from the CTO. • The Backup process will start via a ticket opened to the corresponding datacenter where the backup is required (i.e. - Vazata or Opus).

	• Any backups/restores will be evaluated and reviewed to assess what occurred to cause the restore to be needed, why it occurred, if it can be prevented/corrected in the future, and documented in the SBN Cloud Change Log policy document.

CHANGES TO THIS BACKIP POLICY

This statement may be revised from time to time due to legislative changes, changes in technology or our backup practices or new uses information not previously disclosed in this Statement. Revisions are effective upon posting and continued use of this Software or Services will indicate acceptance of those changes. Please refer to this Statement regularly.

Last revised date: May 6, 2020