Bowling Business Strategies (BBS)

Policy Title: Information Technology Disaster Recovery Plan

This policy is currently in effect and was last reviewed and revised in February 2022.

Section 1: Introduction

Information Technology (IT) infrastructure and services are essential to the staff of Bowling Business Strategies (BBS) to accomplish their work and provide high-quality services to clients.

As a result of this reliance, IT services are considered a critical component in the daily operations of BBS, requiring a Disaster Recovery Plan to assure that these services can be re-established quickly and completely in the event of a disaster of any magnitude.

Response to and recovery from a disaster is overseen by the Managing Principal, working in close partnership with the Operations Consultant and one designated Principal. Together these three individuals comprise the firm's Crisis Management Team (CMT).

This Disaster Recovery Plan presents the requirements and the steps that will be taken in response to and for the recovery from any disaster affecting IT services, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality.

This plan shall be reviewed and updated annually and approved by the Managing Principal.

Section 2: Scope

All BBS staff members work remotely using BBS-issued equipment from workspaces located in several states. This geographic dispersion makes it unlikely that all staff will be equally impacted by a disaster or adverse event. Furthermore, BBS relies on Google Workspace as its sole provider for email and cloud storage, which ensures that all BBS data is protected by Google's suite of security protections. BBS also used cloud-based Microsoft Office 365 accounts for Office software, Zoom and Google Meet for telecommunications, and Squarespace for website administration. The BBS Google Workspace account and other cloud-based software accounts are administered by the

Operations Consultant, in coordination with Managing Principal. All BBS hardware is password protected and all BBS Google Workspace accounts use two-factor authentication.

Section 3: Assumptions

This disaster response and recovery plan is based on the following assumptions:

The safety of staff is of primary importance and the safeguard of such will supersede concerns specific to hardware, software and other recovery needs.

The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be determined under the guidance and approval of the Managing Principal.

Due to the uncertainty regarding the magnitude of any potential disaster, this plan will only address the recovery of systems that are critical for business continuity.

Section 4: Definitions

Backup/Recovery Files: Copies of all software and data are stored in the cloud, which are used to return to a state of readiness and operation that existed shortly prior to the incident/disaster.

Disaster: Any IT incident which is determined to have potential impacts on the business continuity and ongoing operations of BBS.

Crisis Management Team: The CMT is comprised of the Managing Principal, the Operations Consultant, and one designated Principal.

Incident: Any non-routine event which has the potential of disrupting BBS business operations. An incident can be a fire, windstorm, virus, phishing, etc.

Section 5. Crisis Management Team (CMT)

All emergency contact information for the Crisis Management Team (CMT) and all BBS staff is on file with the Managing Principal and the Operations Consultant.

The CMT will be mobilized in the event that a BBS employee experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts. This team will coordinate restoration of these services withthe external vendors or organizations responsible for providing them as necessary.

Section 6: Data Recovery Preparations

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to “pre-disaster” as possible. Specifically, this section addresses the backup and storage practices as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

Backup/Recovery files are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. As noted above, major software applications are provided through cloud-based applications and be re-downloaded easily. All file backups are housed on Google Drive.

BBS requires all staff to store all important files in Google Drive folders that are accessible only to BBS employees. The recovery of data not backed up to Google Drive are not covered under this plan.

Information necessary for the recovery and proper configuration of all application software is critical to assure that applications are recovered in the identical configuration as they existed prior to the disaster. The Operations Coordinator is responsible for keeping the BBS hardware and software inventory up to date, including a record of all administrator passwords and access credentials.

Section 7: In the Event of an Incident or Disaster

In the event of an incident or disaster, the affected BBS employee will promptly notify the Managing Principal, who will in turn notify members of the CMT. In the event the Managing Principal is unable to respond, BBS employees shall notify the designated Principal who sits on the CMT.

Upon notification, the Managing Principal will mobilize the CMT to take appropriate steps to safeguard personnel; minimize damage to any relevant software, files, or hardware; and recover or replace hardware, software and/or files as needed. The CMT is the first to respond to an incident and assess the extent of damage, and coordinates efforts to promptly communicate with all BBS staff members across the firm, as well as important external stakeholders such as clients, subcontractors and vendors.

Ultimately, the CMT will work with affected personnel and vendors to verify restore or replace hardware and software to return it to pre-disaster functionality.

Approved by Jake Bowling, Managing Principal: ____________________ 2/28/22
Signature Date