The Blue Mountains Public Library

Business Continuity & Disaster Management Plan

Introduction

This plan outlines the technological plans to mitigate loss of data and service operations as a result of outage or disaster.

Protocols

Backups

As per MOU with the Town, Schedule C, the Town's IT department supports staff networked computers. This includes maintaining a backup of contents.

1. Staff are required to use the staff equipment including storage of files on a server drive (as apposed to on the actual PC).
2. Any materials created or held on external devices such as cameras or tablets should be transferred to a server drive for storage.

Catalogues

Catalogues such as the library ILS or museum's PastPefect shall be held off site.

1. ILS shall be held in SaaS or server by the company with an assurance statement of backups of files to mitigate loss of data.
2. PastPefect shall be held in SaaS with an assurance statement of backups of files or Town server, for locally held files, to mitigate loss of data.

Business Continuity & Generators

Neither facilities currently have generators. A generator for business continuity will be added to the renovation and constriction plans for each facility. This will not impact current business continuity, but is a plan for future improvements.

Notice of Down Services

While it is the intention to not have a loss of service, a plan for notice is required to inform the public when normal services are not available.

1. Staff shall be able to log onto the website and social media sites remotely and make a notice of closure, power outage, or other.
2. Staff shall be able to remotely access the phone systems to be able to make a temporary voice mail informing of closure, power outage, or other.

Password Storage

1. All staff PCs shall have password updates according to the Town IT Schedule.
2. If a password is lost, shared (inadvertently or purposely), or could otherwise be known by others, Town's IT will be notified immediately. If the user can change the password, this should be done immediately.
3. Shared Passwords will be saved on a common document for access by multiple staff. These passwords will be regularly updated. (E.g. Staples, Social Media, Deputy Scheduling).

Website

1. The website shall be maintained by third party who provide assurance of backup of files.
2. Copies of electronic documents uploaded to the website shall be available on the BMPL server (and not only stored on website).

CEO Passwords

The CEO shall maintain a list of confidential passwords on the CEO personal drive. This shall be entitled "1.1 Confidential". In the event of the CEO files needing to be accessed, the Town IT can retrieve this file for use by the Board or Acting CEO.

Update to Plan

This Business Continuity & Disaster Management Plan will be updated every two years, on the even year, or as protocols change.