GREEN GOLD LIBRARY CONSORTIUM
DISASTER RECOVERY/BUSINESS CONTINUITY POLICY

Critical data is defined as "the data that is critical to success" in a specific business area. For the Green Gold Library Consortium, critical data includes:

- Budget
- Board Minutes
- Overdrive Records,
- Financial Records
- Email Correspondence (*Through Shreve Memorial Library; covered under their Disaster Recovery/Business Continuity Policy)*

Data is backed up periodically on a set schedule to ensure recovery in case of a disaster. Frequency is determined based on equipment usage and data priority. The storage of most backups is housed in a separate facility site from its primary location for safekeeping. Periodic testing and verification of backup systems takes place on a quarterly basis.

The use of antivirus software on staff PC's is essential and required. The Board, through Shreve Memorial Library's IT Department, is responsible for staying abreast with the latest antivirus software available. The application of software updates are necessary and must be carried out in a timely fashion. In the case of a disaster, contact the following in descending order to ensure business continuity:

1. Chief Financial Officer
2. Shreve Memorial Library's IT Department Head
3. Green Gold Library Consortium Officers

Approved March 18, 2022