Electronic File Backup and Security Policy (DRAFT)

1. Overview and Scope

The purpose of this document is to define the Data Security Policy of the Lake Union Conference ("LUC") Planned Giving and Trust Services ("PGTS") policy on electronic file backup and security. The Policy provides guidance in compliance with NAD Working Policy BA 70 10 6 and PGTS Standard 23b "Electronic files held in a fiduciary capacity and other legal documents are properly backed up and secured per organizational policy approved by the governing board or committee and legal counsel" and applies to the PGTS Department.

PGTS is often the custodian of personal data related to trust services provided to members within LUC. Data security focuses on controlling unauthorized access to data. Violations could jeopardize our ability to provide service, create monetary liability, reduce credibility, and inhibit the effectiveness of our ministry.

2. Security and Backup Policy

In compliance with PGTS Standard 23:

1. Data will be accessed on the principle of least privilege that is required to complete a task.
2. Usernames and passwords must not be shared, revealed, or allowed to be discovered due to carelessness.
3. Access to the network/servers and systems will be by individual username and password.
4. For remote access two-factor authentication is required.
5. Where possible, no one person will have full rights to any given system. The IT Department will control network/server passwords and system passwords will be assigned by the system administrator(s).
6. Data will be securely backed up at least daily per guidance from IT.
7. The IT Department will test backups at least quarterly.
8. File systems of servers and computers will have the maximum security implemented that is possible. Where possible users will only be given read rights to directories; files will be flagged as read-only to prevent accidental deletion.
9. Role-based access control will extend to third-party applications where possible.
10. The IT Department will implement policies, standards, guidelines, and best practices for securing and backing up electronic data.
11. Physical PGTS files must be physically secured to prevent theft, tampering, or damage in compliance with PGTS standard 23a.