REVISION HISTORY

New document adopted **2/10/2016.**

BACKGROUND/PURPOSE

To safeguard personal and financial information about congregants collected and stored at UUCWC.

POLICY

Congregants' personal and financial information, including pledge and contribution details, are considered private, and should be accessible ***only*** on a "need to know" basis.

It is the policy of UUCWC that individuals with access to congregants' private information be limited to those authorized to use it. The Finance Committee has the authority and responsibility to develop procedures for carrying out and enforcing this policy.

In addition, the Finance Committee has the authority and responsibility to develop procedures intended to ensure a smooth transition as those authorized persons relinquish their roles and new persons are named in their place.

The Finance Committee is accountable to the Board of Trustees for the implementation of this policy.

PROCEDURES

I. Persons/ Roles Requiring Access

The following people / roles should be the only individuals with access to congregant information:

1. Chairman of the Stewardship Committee
2. Canvassers & Canvass Committee as necessary
   The Stewardship Chair may exercise discretion in sharing information with canvassers/ committee members to assist in committee responsibilities (e.g. - a canvasser should be able to answer canvassee questions on prior pledge details)
3. Treasurers and Assistant Treasurers in order to reconcile deposits
4. Staff as needed to perform their roles including maintenance of congregants' records
5. Minister

II. Congregant /Stewardship Database Access & Administration:

ICON CMO

UUCWC presently uses the ICON CMO (Church Management Organization) database system to record and maintain congregant membership and financial information.

1. Access and support of the database system should be limited to the following persons:
    a. The Chairman of the Stewardship Committee – who should also be system administrator
    b. Treasurers and Assistant Treasurers, in order to reconcile deposits
    c. Staff as needed to perform their roles including maintenance of congregant records
    d. Minister
2. Newly elected persons in roles noted should be granted access as required for the tenure of their roles
    a. Retiring persons in these roles should relinquish/ have their access revoked
    b. Passwords and all forms of access should be kept confidential and changed at the time that roles change

Google Drive

The financial team also employs cloud storage on a Google Drive to share reports and check images to facilitate reconciliation of bank deposits. Access and support of the cloud storage and any other financial storage or communication mechanisms should be limited to the following:

a. Chairman of the Stewardship Committee – who is also administrator of the Google account
b. Treasurers and Assistant Treasurers in order to reconcile deposits

Check and other aged information on the Google Drive should be deleted after no more than three months.

E-mail Communications, Reports & Other Communications

All communications involving congregant private information including financial information should adhere to the "need to know" standard:

1. Financial e-mails ("weekly batches") that share church deposit information including, but not limited to congregant check details should include ***only*** the following persons:
    a. The Chairman of the Stewardship Committee
    b. The Treasurer (who needs only totals – efforts should be taken to mask congregant details if possible)
    c. Assistant Treasurers

Password Requirements

Passwords must be used to protect sensitive data. Passwords should be used for applications, services and individual documents. Passwords should be of 8 or more characters long and should have complexities like upper case letter, lower case letter, special characters and numbers.

UUCWC Password Requirements*

1) Password Length is 8 or more characters minimum
2) Password must have all the below four groups of character types.
   - At least one uppercase letter (A,B,C, ……Z)
   - Lowercase letters (a, b, c, …..z)
   - At least one numerals(0,1, 2, …9)
   - At least one special, non- alphanumeric character (!,@,#,$,%,* etc.)

Passwords must be changed at least once per quarter.
Passwords must be changed when an individual no longer holds a position requiring access to sensitive data.

*Exceptions to these requirements are allowed if they are not permitted by the application or service.

Access Review

The Finance Committee will conduct an annual access review. The review will assess whether the requirements stipulated in this document are being followed. The results of the access review will be shared with the Board of Trustees, the minister, and any independent auditor retained by the congregation.

Definitions

Congregant personal information includes identifying information such as name, address and phone number.

Sensitive congregant information includes:

- Credit card information
- Social Security number
- Date of birth
- Pledge/contribution information
- Health-related information
- Personal counseling information

Document prepared by: Joe Schenk, chair, Finance Committee