First Unitarian Society of Milwaukee
Staff Policies Manual

Computer & Network Access

November 8, 2023
Shari Wright
Information Technology Team

Purpose

This policy is intended to make secure access to First Church's computers and networks, either in the First Church building or on First Church cloud networks[i] using passwords and, in some cases, second-level authentication. A password is the front line of protection of our electronic information. Everyone who needs access to use the First Church information systems must follow this policy to select and secure their passwords, including the user authentication policy.

Scope

The scope of this policy includes the staff of First Church and lay leaders that require access privileges to any church-owned computer, application, cloud application, and the network.

User Authentication Policy

Every staff member may be assigned a unique user account and a password for access to our computers, and the network, as well as a unique user account for our email system and our cloud applications. The accounts assigned to staff are provided by the Information Technology Staff Team (IT Team.) This policy will be enforced by the IT Team through the application login process.

Accounts created by staff for First Church's cloud-based applications must follow password policies where sensitive information[2] is stored (such as Constant Contact and the Realm database). This policy includes incidental or temporary applications which store sensitive information which the admin staff team does not manage (such as GiveSmart, Eventbrite or any online form collecting information.)

Passwords should not be shared with anyone. Accounts with sensitive information, such as credit card information or personal contact information, cannot be shared with lay leaders. Passwords are to be treated as sensitive, confidential information. If someone requests password(s), staff must inform him or her that we cannot provide that information per our policy.

If you suspect an account or password has been compromised, report the incident immediately to the IT Team and change all related passwords.

Password Requirements

- All network passwords and Office 365 email and accounts are required to create a complex password with secondary authentication.
- The password for all cloud-based applications with sensitive information must be changed every 180 days unless the password is protected by secondary authentication.
- If multifactor password protection[3] is enabled for a password, set it up using a personal phone or email address that is not shared with anyone else.
- New passwords cannot be the same as the previous passwords.

Enforcement

Any employee found to be in violation of this policy will be reported to their supervisor and may be removed from the account access until the user reviews the policy and a plan to remedy the situation is created with the supervisor and IT Team staff member.

Related Board Policies

This policy supports the First Church Board of Trustees (BOT) policy 4.6.8 which states" the Senior Minister shall not allow physical and electronic assets and data to lack reasonable protection, including from cyber threats." This BOT policy was approved in April 2019.

---

[1] Cloud services are defined as networks of remote servers hosted on the internet to store, manage, process data, and execute applications, rather than a local First Church server or personal computer.

[2] Church member's information is considered sensitive data. This could include customer names, home addresses, payment card information, social security numbers, emails, application attributes, and more.

[3] Multifactor password protection can be set up (if enabled) with your personal phone or email by logging out or accessing your account with another computer or to reset your password if you forget it.

First Unitarian Society of Milwaukee
Database Software Security Policy

The objective of this policy is to protect the database information from a security breach, protect the integrity of the data, and provide a way to keep the data up to date.

The definition of our security information includes:

- Financial data
- Personal information, including notes
- Members' private information
- Non-member contact information
- The database structure, system messages, and group listings

The Primary Administrator will be responsible for the database structure, assign additional rights to the users per this policy, and monitor the integrity of the data. In developing the structure, s/he will confer with, and take into consideration, appropriate constituents.

Policy:

1. The Primary Administer will be designated by the Director of Administration.

2. No more than two supporting administrator accounts will be created. In addition, the Director of Administration will have access to the Primary Administrator's full credentials as a backup.

3. The Primary Administrator will develop policies in consultation with appropriate staff.

4. All users requesting access to security information must apply to the Primary Administrator for additional rights. Requestors may only be given additional rights to access the data information that is related to their job responsibilities.

5. All users requesting security information must hold a staff position, or be a member who belongs to a staff-led, First Church group.

6. All users with additional rights will seek pertinent additional software training from the Primary Administrator, and will abide by the policies.

7. Any data errors, deletions, or security breaches must be reported to the Primary Administrator immediately with the time, date, and nature of the incident.

Database (Realm) User Security Request

If your position requires access to areas of the database besides your group leadership access to manage the group, then you need to request additional security access. If the security access below says "Manage," you will have authority to add, edit and delete. By filling out this form, you acknowledge that you have read the security policy printed on the back.

Your name:___Jean Johnson_____
Your job title or leadership position__Director of Administration_____
Describe responsibilities of your job that requires access to the database.

1) Financial operations and management, including pledge fulfillment forecasting and reporting, deposits and audits.
2) Vetting Facebook Group member requests.
3) Providing non-financial information about members to Nominating Committee and other leaders.
4) Finding members for leadership positions for teams and projects.

Check one or multiple security access requests:

Manage Individuals

- ☐ View visitor and member profiles
- ☐ Add individual profile
- ☐ Delete individual profile
- ☐ Manage profile fields
- ☐ Manage notes
- ☐ Manage private notes

Manage Giving and Pledges

- ☐ View giving summary on dashboard
- **X View individual contributions**
- ☐ Enter gifts
- ☐ Enter individual's pledge

Manage Groups

- ☐ Create groups
- ☐ Edit groups
- ☐ Delete groups

Manage Events and Check-in

- ☐ Manage events
- ☐ Manage registration for events
- ☐ Manage check-in (kiosks)
- ☐ Launch check-in (kiosks)

Manage Volunteers

- ☐ Manage Stills/Interests
- ☐ Create Serving Teams/Roles

Your supervisor or staff team Signature_____