

# MemberLink Security

## Overview

MemberLink is an information system designed to save time in the administrative tasks regarding the membership of your church. It is also intended to be a tool to help church members keep in contact with each other.

A MemberLink system is accessed through the Internet using a web browser and is navigated similar to a web site. All information is stored in an Oracle style database.

## Security is High Priority

The security of your information is one of our highest priorities! We have taken the following steps to insure the safety of your information.

### *Secure Server*

1. All security updates for the server are installed as they become available. (Usually updates are available hours after the security concern has been discovered.)
2. The server has only the necessary ports open to the Internet. Extra ports that are often used by malicious people and programs are closed.
3. All information is encrypted with 128-bit encryption when it travels through the Internet. This is the same encryption banks, online merchants and e-commerce web sites use.

### *Secure Access*

1. Users must log in to access the MemberLink information. Only people already in the MemberLink system can receive a username and password, and each person must be approved by the MemberLink administrator.
2. Sensitive information is reserved for people with extra access. This is allowed on a per person basis.
3. Pages are not allowed to be stored on your computer by your browser (the cache). This is often done for faster access to web pages, but is not allowed when accessing MemberLink information. Each time you request a page, your username and password is verified.

### *Secure Authentication*

1. Once logged in, cookie information is stored with a unique token and the user's id number. Both of these are used to verify the person for access to any page. A person may be able to modify their cookies to have the user's id number set, but the token is created each time a user logs in, and is virtually impossible to match.
2. If a user tries to log in and fails five times in a row, that username is temporarily inactivated. This helps to stop people from guessing a password if they find out someone's username.
3. (optional) Users must type in a randomly generated sequence of letters displayed on the log in screen. This stops script programs that try to guess passwords.
4. (optional) Passwords must pass strict rules based on the CrackLib library: they can not be based on a dictionary word, must contain many different characters, and must be a certain length. For more information see: <http://www.php.net/manual/en/ref.crack.php>

## Things You Should Do to Keep the System Secure

1. Never tell anyone your username or password.
2. Do not write down your username or password. If you must write down your password, do not write your username on the same piece of paper, or with any instructions on how to use that password.
3. Change your password frequently. Guided Vision recommends passwords be changed at least twice a year.
4. Do not pick a guessable password such as your spouse's name, your child's name, or your birthday.
5. Always click "logout" when you are finished. This removes the cookies from your computer and "locks" the system. As an added precaution, close your web browser when you are done.