Computer and Internet Use and Security Agreement

Messiah Lutheran Church

All Staff and volunteers of Messiah Lutheran Church who are authorized to have access to church technology and the internet via the church's networks are required to use their access in a Christian, legal, and informed way, conforming to network etiquette, laws and courtesies.

This Agreement should be signed prior to using any computer equipment or networks owned or connected to Messiah's system. All users are required to read the current Computer and Internet Policy prior to signing this agreement.

Computer systems covered by this policy and agreement not only include~~s~~ systems owned and maintained by the church but also all other computers or systems physically or electronically connected to the church's computers and networks.

I ________________________________, have read the current Computer and Internet Use and Security Policy and agree to abide by the terms and requirements of this policy. (Please provide signed agreement to the Congregation's Vice-President.)

Signed ______________________________ Date ____________

Computer and Internet Use and Security Policy

Messiah Lutheran Church

This Computer Use Document and the attached Computer Security Policy are to be annually reviewed by all users of Messiah Lutheran Church computer systems. This Agreement should be signed prior to using any computer equipment or networks owned or connected to Messiah's system.

Overview: Staff and volunteers of Messiah Lutheran Church who are authorized to have access to the Internet and church technology are required to use their access in a Christian, legal, and informed way, conforming to network etiquette, laws and courtesies.

Messiah Lutheran Executive Committee Responsibilities: The Executive Committee will:

- Annually review the current *Computer and Internet Use Policy* and recommend changes to the Church Council for approval.
- Recommend the extent to which staff/volunteers may use Church computers and/or Internet to accomplish job responsibilities. Any questions about the appropriateness of a particular use of the Internet should be discussed with members of the Executive Committee.
- Confirm the appropriateness of using the Internet and/or church computers for professional contacts and career development activities during office hours;
- Approve and confirm training required of staff using the Internet and/or church computers and the work time that may be used to practice/acquire skills needed to effectively access and use the Internet and/or church computers.
- Determine requirements for installing a pornography filter or other ***I***nternet blocking software.

All Staff and Volunteers who use Church computers, equipment, systems and networks will annually review and sign the current *Computer and Internet Use and Security Agreement***.** The signed Agreements will be maintained in the Vice President's Current Folder.

The Internet is not a secure communication channel and should not be used for sending or receiving confidential or sensitive information.

Use of the Internet and computers is a privilege, not a right, which may be revoked at any time for inappropriate conduct. Misuse of Internet access or computers by a staff person may result in other disciplinary action, including but not limited to, termination of employment. Examples of inappropriate conduct include, but are not limited to: use of inappropriate, offensive or abusive language in either public or private messages; unlawful activities; defamation; infringement of copyrights; misrepresentation of oneself or the Church; logging on or accessing pornographic, sexually explicit, violent sites or materials, accessing gambling sites, initiating viruses, and sending messages that might result in congestion or disruption of networks and systems.

Staff members and other users should notify the Pastor or church officer if she/he observes or becomes aware of any inappropriate conduct or use of the Internet and/or church computers by church staff or others.

The Church Vice President will initiate an investigation into allegations of misuse. Results of any investigation will be presented to the Executive Council for action.

All programs, files, and E-mail stored on Church systems are property of Messiah Lutheran Church. Staff use of church technology is not private. Messiah Lutheran Church reserves the right to monitor all users of the Internet and/or church computers at any time. All users must abide by security policies, procedures and guidelines, and are to refrain from practices that might jeopardize the church's computers, data, network, system security or work in general. Staff must guard against computer viruses and security breaches of any kind. Staff who use the Internet may not transfer or install any software or files from the Internet to any church computers or information systems except in consultation with appropriate technical staff (i.e., no downloading of software, programs, games, etc.).

Although church staff is specifically mentioned throughout this policy, the same provisions apply to church volunteers and other users of church IT systems. This policy applies to all Internet/computer use on church premises and use of church property outside of the church premises. *

- Clarification - Some staff members or church volunteers may supply or use their own Internet access provider, software or even computer, or may use church property off site. It is important to note that this policy applies even if some, or all, of the computer equipment/Internet access is not supplied by the church on its premises and to use of church property off site.

Computer Security Tips and Policy

Tips for Computer and Internet Safety

By better understanding security threats associated with the use of computers and the internet, and by understanding the manner in which these threats are exploited, we can better protect our congregation, our congregation's information, computers and computer files.

Each and every day, people are trying to gain unauthorized access to computers, applications, confidential information, and other valuable electronic assets all around the world. In some cases, the people trying to gain this access might even be known to you; some can be your co-workers or other people that you trust. Unauthorized access to computer resources can result in the loss or corruption of vital information or damage to the reputation of our congregation or people within it. These tips are not meant to cover all aspects of computer and information security, but are basic guidelines to begin to secure computers and information assets against common threats. The tips covered are in relation to the following topics:

- Physical Security
- User names and passwords
- Computer security policy
- Social Engineering
- Phishing
- Viruses and Spyware
- Using Public Computers
- Backups
- Network Security

Physical Security

Prevention against information theft best begins with securing the physical assets within our organization. Physical security refers to protecting the physical access to a PC, laptop, or server. Any other virtual security measures prove worthless if an ill-meaning individual is able to walk up to a logged-on system, shoulder-surf authorized users, or browse a laptop full of contact information and other unprotected data. There are several quick things that you can do to protect against this threat:

- Ensure you log off or lock your machine whenever you leave it unattended. A quick press of the Windows Key and L key at the same time will lock your machine before you walk away from it.
- Windows' built-in screen saver offers the ability to automatically lock your system and require anyone approaching it to enter a valid password to access the system, should it remains unused for the period of time you specify.
- Apple computers have similar "locking" capabilities.

- When traveling with a laptop, or handheld computer, it’s imperative that you keep these units within your view at all times or secure with ***a*** lock that attaches to any notebook or other hardware equipped with a lock slot. In the event that a portable system is stolen, the thief would be able to hack the unit at leisure, potentially enabling him or her to assume your identity, access all your system’s data, log on to the network, access all the organization’s data, and worse.
- Ensure that servers are kept in a secure location within the building that has restricted access to them. Flash drives are a quick way for thieves to steal data off servers or infect them with a virus or spyware.

Protecting your user name and password

When combined, a user name and password create a powerful combination in allowing access to sensitive information. A user name and password combination should be utilized to protect all personal and networked computers. The user name is the electronic identity providing the ability to log on to your PC or laptop, access network resources and data, surf the Internet, and send and receive e-mail. Paired with your user ID, the password is the key to your private digital assets similar to the key to your home. Account names can often be guessed very easily, which makes protection of your password(s) even more critical and should be much more difficult to crack. Here are several tips to securing your passwords:

- Never provide your password to anyone.
- Never write your password on paper.
- Always create complex passwords to help prevent committed hackers from cracking them. Passwords should include letters and numerals, and when possible, special characters such as the pound sign (#) or ampersand (&).

  Weak passwords to avoid include those based on:
  - Your, your spouse’s, your children’s, or your pets’ names
  - Social security numbers
  - Anniversary or birth dates
  - Favorite sports teams
  - Words in the dictionary
  - Avoid using versions of these weak passwords by spelling them backwards or altering them by simply adding numerals to the beginning or end.

Policy for Internet and Computer Use

Computers are used for correspondence, bookkeeping, members’ personal data, emails, website creation and research, as well as a variety of other important functions by staff and volunteers. It is important to safeguard the use of computers and the Internet. We have adopted an Internet and computer policy as an important step in this safeguard process.

This policy will be reviewed annually by the congregation council or IT committee. This policy sets forth procedures for those authorized to use computers and the Internet, and what uses are limited or prohibited. Our policy will make clear that computer and Internet access are privileges; their use is not private and is subject to review at any time.

Social Engineering

Social engineering is a tactic used by people who intend to steal data from you or misuse your identity. Social engineering attacks rely on a person's nature to trust people and to help one another when persuasively convinced that the individual requesting the information is well intentioned. These efforts to con you will include attempts to get you to reveal your account names, passwords, and other sensitive personal information. These individuals will often pose as customer service representatives or even IT support staff. This information will then be utilized to gain unauthorized access to systems and data. You should never provide sensitive account or personal information to anyone over the phone if you cannot verify who they are and where they are calling from.

A major reason for the increase in sales of paper shredders is due, in part, to one form of social engineering called "dumpster diving". Rifling through trash for account or personal information, has proved to be a very successful means for these ill-willed individuals to obtain this information about you.

Phishing

Phishing is a relatively new threat that has gained a lot of popularity lately in getting people to reveal sensitive information. Phishing relies upon purely electronic means to attempt to obtain this sensitive information. The most common method is an e-mail message that appears to come from the victim's bank, online store, or other financial companies. These fake messages typically state there's been a problem and the victim must click on a provided link to confirm or update account information. Victims end up submitting their account information directly to the scammer and thus compromise their identity.

Phishing attempts continue to improve and appear, at least on the surface, to be legitimate. They contain real company logos, apparently valid URLs and come from seemingly legitimate email addresses. The logos are typically stolen from the real company's web site; the URLs are typically redirected to web sites unassociated with the actual organizations, and the email address sources have been forged.

In order to avoid phishing scams altogether, never provide sensitive, proprietary, or confidential information; or account, password, or financial information in response to an e-mail or instant message. Also, pay close attention to the address information for the web sites you visit. Always confirm that account or other sensitive information you provide is being entered on the proper organization's Web site and that you haven't been redirected to another location. Many phishing scams might include a URL that appears to be from yourbank.com, but instead directs to a fake Web site owning a suspicious or numeric URL. This is an immediate sign that you shouldn't provide any information.

Viruses & Spyware

Always remember not to click on unknown attachments received in unsolicited e-mail messages, particularly those from unknown persons and even on attachments received unexpectedly from people you do know. Often times, individuals can be sending a virus in a file and not even know it. If you are ever in doubt, confirm that this person meant to send you a file, link or image in an email or instant message. If there is no way to confirm with the sender, then make sure to scan the file with any leading anti-virus application.

Never install programs found on unknown websites on the Internet; you should only download applications from trusted Web sites at home and use only authorized programs at work. In addition to viruses, spyware and adware programs may be contained in these downloaded applications. Spyware and adware are nuisances that will consume unnecessary system and network resources, potentially monitor everything that you do on your computer, and often report your behavior to advertisers or other third parties. In reporting this behavior back, these programs can also send confidential information, such as your bank account and credit card numbers.

Whether at home or at work, every PC and server should be configured to run Anti-Virus and Anti-Spyware software to scan new files as they are placed on your system, monitor changes to your system by newly installed applications, and scan all files on the entire computer at least once a week. (Note: There are several commercial Anti-Virus programs that are recommended for use from Symantec, McAfee or Trend Micro. For your personal computers, two free programs from AVG and Avast are also recommended for use. Popular antispyware applications include Lavasoft Ad-Aware and Microsoft Windows Defender Anti-Spyware.)

You should be sure to check for periodic updates for both Anti-Virus and Anti-Spyware applications to ensure that your system is protected against all of the most current threats on the Internet.

Using Public Computers

Public computers offer no guarantees of security or privacy of any information that is accessed while using them. This includes any email that you may have read, any credit cards that you used while shopping, or any passwords entered. You should only use public computers when absolutely necessary or for general web browsing. If you enter any sensitive information while using a public computer, be sure to empty the cache for the browser, delete any history within the browser, and clear any information that may have been stored on a form that you filled out. For more information on how to stay safe while using a public computer with Internet Explorer, please visit this web page provided by Microsoft.

Backups

Be sure to backup essential data on your computers. It is recommended that all critical files be backed up on a regular basis to protect against loss of data in event of a system crash. Backup software is included with all versions of the Microsoft and Apple operating systems. This can be used to protect your data by moving it to another computer, a set of DVDs, an external hard drive or a USB memory thumb drive.

Network Security

A security approach that leverages several layers is the most effective in protecting the computers and information that is stored on them. Firewalls, Internet web filtering software, wireless network protection and several other technologies should be reviewed for applicability of use within your organization.

Suggestions:

If you have suggestions to improve Messiah Lutheran Church's Computer, IT, Internet, or Network systems or services, please direct you suggestions to our IT personnel or the Council Vice-President.