Technology Oversight Policy

Revision 1

Purpose: To establish rules, regulations and oversight for the use of Christ Lutheran Church (CLC) owned and operated information technology resources.

Scope: CLC provides different levels of access to electronic information resources, including networks, software, and equipment to its leadership, staff, membership and visitors.

Responsibility: The Council shall make all decisions with respect to the enforcement of this policy.

Policy:

1. Administrator Usernames, Passwords and Access Points:
    a. The Technology and Communication Committee (TCC) Chair shall maintain a document (herein unpw doc) that contains all administrator usernames and passwords for all CLC owned devices, websites, applications, and operating systems. The document shall indicate usernames and password entry points and include a description for each. A copy of this document shall reside on the CLC Server computer. This document shall be accessible via password and shall be made available only to the TCC Council liaison.
    b. The TCC Chair and TCC Council liaison shall review the unpw doc every year in February (after the Annual Meeting) and make any changes deemed appropriate.
    c. CLC shall maintain a relationship with a 3rd party technology vendor that shall have administrative access to the CLC Server and Firewall, when granted permission by the TCC Council liaison, TCC Chair or Council President.
    d. The TCC Chair shall be allowed to share certain admin passwords with select individuals who are responsible to help administrate particular areas of CLC technology.
2. Internet Access:
    a. CLC maintains a computer network and Internet access to help support its primary mission. Using the network for occasional access to the Internet for personal purposes is not specifically prohibited. However, violations of Internet use include, but are not limited to, accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language and/or content.
    b. Users should make economical and wise use of computer and network resources. Users should report suspected unauthorized use of resources to a member of the Executive Committee. Theft, failure to observe copyright laws, and/or tampering with any computer system or network device will place violators in jeopardy of losing privileges as well as possible criminal prosecution. Each incident will be handled on a case-by-case basis and may be referred to an appropriate authority.

3. Wireless Network Access & Usage:
    a. CLC's wireless network infrastructure has been installed to provide connectivity options for general network access within the facility. The primary mission of the wireless networks is to provide general network access for staff and membership.
    b. CLC provides two wireless services. One is meant for the membership, it is accessible from anywhere within the facility, and its access code is made public. The second is available for staff and leadership, it is available only in the office area of the facility, and its access code is kept private.
4. Electronic Mail (email):
    a. In general, use of CLC email services is encouraged subject to the following conditions:
        i. Email services are to be provided in the support of the purpose and mission of CLC.
        ii. Users of CLC email services are to be limited primarily to CLC staff and leadership for purposes that support the mission of the church.
        iii. CLC email services may not be used for: unlawful activities; commercial purposes not under the auspices of the church; personal financial gain; or uses that violate other CLC policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment.
        iv. Email users shall not give the impression they are representing, giving opinions, or otherwise making statements on behalf of CLC unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the church. An appropriate disclaimer is: "These statements are my own, not those of Christ Lutheran Church."
        v. CLC technical resources may not be used to:
            1. Perpetuate chain email letters or their equivalents - This includes letters that require the recipient to forward an email to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal. Emails that are part of a multilevel marketing or pyramid-selling scheme, sometimes known as "Ponzi schemes," are generally illegal and are specifically forbidden under this policy.
            2. Create and/or send "spam" - Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication.

3. Send or encourage "letter bombs" - Letter bombs are extremely large or numerous email messages that are intended to annoy, interfere with, or deny email use by one or more recipients.
4. Practice any activity designed to deny the availability of electronic communications resources - Also called "denial of service attacks," these activities deny or limit services through mail bombing, malicious executables such as viruses, threatening a virus, or opening a large number of mail connections to a mail host or SMTP relay without authorization or permission.

5. Security:
    a. No user shall attempt to access any service or resource to which they have not been explicitly authorized access by the appropriate CLC authority. All network access ports are provided for use with a single computer system. No router, wireless access point, hub, or other network device may be installed without prior review approval from the Technology and Communication Committee. Users of the network shall not perform any activity which disrupts network or server resources, impedes or prevents network or server access by others, or attempt to access private data of others. Examples include, but are not limited to, port scanning software, packet sniffers, mail bombing, ping flooding, SMURF attacks, and/or SYN flooding. Users found to be in violation of this policy will be denied access without prior notice.
    b. In order to ensure the security of CLC's network and the systems attached to that network, the Technology and Communication Committee has implemented security devices which will ensure that the network is adequately protected from malicious traffic to/from leadership, staff, membership and guests. These devices will block traffic identified as viruses, worms, and exploits.
6. Rights and Privileges:
    a. Having a network account is a privilege, not a right or entitlement. An individual is assigned an account for use while conducting activities related to the mission of CLC. The holder of an account may not share access information that would enable use of an account with anyone. Any account may be revoked temporarily or permanently if a user of CLC information technology resources violates public law or CLC policy.
        i. The CLC network shall be configured to force users to change their network password(s) at minimum once every six months.
7. Membership database protection:
    a. CLC shall not make available its membership database to any third party except as provided for within this policy.
    b. CLC may provide its membership database to third party vendors or agents of CLC as long as that provider respects CLC policy. An example of an acceptable third party would be the CLC website application provider, which hosts the CLC online membership directory.

8. No Expectation of Privacy:
    a. CLC reserves the right to access, monitor, copy, intercept, inspect, or audit with or without notice all operation or use of CLC technology assets and information.
    b. Traffic to and from personally owned devices connected to the CLC Network are subject to no expectation of privacy.
9. CLC Server Backup:
    a. The CLC Server shall be fully backed up on a daily basis (this includes the operating system, programs and data). For disaster recovery purposes a full system backup shall be created upon installation of the new Council. The TCC Chair shall take it off site to a secure location known and accessible to the TCC Council liaison.

Revision History:

Revision 1: Approved December 9, 2014