TECHNOLOGY ASSESSMENT and REVIEW

McKNIGHT CROSSINGS CHURCH of CHRIST

(A NON-PROFIT ORGANIZATION)

June 2020

Prepared by:
M. Bret Blackford

To the Administrative Elders of:
McKnight Crossings Church of Christ
2515 S McKnight Rd, St. Louis, MO 63124

June 2020

Don Fitzgerald
Brad Stevens
David Weiler
Administrative Elders
McKnight Crossings Church of Christ
2515 S. McKnight Road
St. Louis, MO 63124

Don, Brad, and David;

The Administrative Elders recently engaged me to document the information technology (IT) currently in use at the McKnight Crossings Church of Christ ("Church" or "MX") and to provide any recommendations on best practices. Attached is my report with details on the environment and some suggested recommendations. However, please consider this the beginning of an ongoing conversation about the use and risk of technology at MX. Technology is a fluid and dynamic landscape and we should periodically revisit the discussion on how it is implemented.

In summary, the environment is well architected and maintains an appropriate level of confidentiality, integrity, and availability (CIA). Some areas of improvement were recognized and it is recommended that the following be considered (items are more fully explained in the Recommended Enhancement section of the attached report):

1. Classify data and determine what is "sensitive"
2. Provide periodic employee security training
3. Adopt a security and acceptable use policy (AUP)
4. Backup and secure data

As part of this engagement I plan to make myself available to assist with implementing the recommendations noted above, should the Admin. Elders wish to move forward. I am also available to provide any other assistance in response to the information presented in the attached report or other concerns regarding MX IT security.

Regards,

M. Bret Blackford

M. Bret Blackford
bBlackford@McKnightCrossings.Org
314-402-7086 : mobile

Contents

I. BACKGROUND

Federal Tax ID: 43-0910590
MO Sales Tax ID: 12553450

McKnight Crossings Church of Christ ("MX" or "Church") is a church registered as a nonprofit organization which is tax-exempt under section 501(c)(3) of the Internal Revenue Code. MX also supports various foreign and local ministries and operates the Sow & Grow Christian Preschool (http://mcknightcrossings.org/preschool). The Church owns the building at 2515 S McKnight Road which is the primary location of operations. The building is also periodically used by civic organizations (Saving our Babies and Family Engagement) and as a polling place for elections.

As we consider what controls may be appropriate we need to evaluate the risks specific to the Church as well as associated organization (such as the preschool and others which may use the facility).

II. CURRENT STATE

Staff: See **Exhibit A**

Networking:

MX does not specify a computing platform but allows ministry leaders to use the technology they feel is best suited for their needs. This necessitates the MX infrastructure to accommodate various hardware and software: Apple iOS, Microsoft Windows, iPhones, iPads, MacBook's, Intel computers, etc. Being platform agnostic allows flexibility in tools but the lack of standardization makes troubleshooting and diagnosing technology problems trickier and also complicates cross training.

The *MX-main* wireless network (discussed below) and the wired network in the office allows connected devices to intercommunicate. This shared network allows shared devices like printers and network storage. Access is limited to MX staff.

Wireless Networking:

MX relies primarily on the wireless network. The current wireless infrastructure is built on Cisco Meraki hardware, which provides cloud management. A network of 4 wireless access points (APs) are utilized throughout the MX building to provide facility-wide wireless access. Cloud management costs $65 per device per year, or $260.00/year.

Meraki CUSTOMER: 2988-2114

AP locations	**AP Name**	**AP Model**
Office	MR34-Office	MR34
Foyer	MR34-Foyer	MR34
4th Floor	MR34-4thFloor	MR34
Baptismal	S-MR18-	MR18

These are business grade devices and are cloud managed, meaning they can be monitored and configured remotely. The cloud dashboard also provides detailed information on usage, internet client traffic, and notifies of any questionable user access. To maintain segregation on the wireless network we have the following SSIDs (networks) for user access:

SSID	**USE**
MX-Main	limited to MX staff
MX-guest	for visitors
MX-VideoSecurity	for security cameras
MX-equipment	for IoT devices (smart plugs, thermostats, etc.)

Using the various SSIDs noted above provides greater security by keeping MX staff, guests, and equipment separated and secure (via passwords and black/white lists).

Wired Ethernet Network:

The MX office area is wired with cat-5 Ethernet in all work areas. All cat-5 cables terminate at the locked computer room in the MX office hall. The main internet line is routed to this room and feeds the gigabit Ethernet switch. The wireless access points also terminate at this switch so all wireless connections on *MX-main* and all wired connections at the office are able to communicate securely.

Additional secondary Power over Ethernet (PoE) gigabit switches are also located in the electrical closet in the MX building foyer and on the 4th floor storage area. We utilize PoE to power the various Wi-Fi APs in these areas.

Internet Provider:

We are able to source our internet from several providers, which gives us better competitive pricing. Currently we use AT&T internet and receive fiber to the building. By utilizing AT&T business fiber internet we are able to maintain consistent internet speeds. Our current plan allows for 100Mb download speed and 25Mb upload speed at a rate of $53.50 per month (including tax and fees).

Plan: AT&T Internet for Business - Business Fiber 100
Account: 252700614
ID: 12345a@att.net

Telecommunications:

With the exception of the emergency phone in the elevator the MX building uses voice over IP (VoIP) phone systems. Going VoIP makes us provider agnostic by freeing us from the local carrier – AT&T. We can now shop price and service, as long as we have internet service.

Analog Lines (for elevator) @ $40/line/mo:
314-963-1136: elevator dedicated line
ATT Acct. No.: **252700614**

Digital VoiP Lines (Ooma) @ $15/line/mo:
314-380-0396 : Sow-n-Grow
314-396-2297 : MX-Church
314-962-7056 : Ring Group

https://office.ooma.com
Main MX Number: <== 314-962-7026
Ooma Customer Care: 1-866-939-6662

Software and Data

Philosophy: Wherever possible the goal is to utilize Software as a Service (SaaS). A SaaS model removes most of the technical support headache away from the end user. It also greatly assists in data backup and reliability of service (minimizes downtime). Most SaaS applications also allow usage from any connected device, freeing users from a geographic location (office desk).

As a non-profit organization we have taken advantage of several special discounts offered by various corporations and organizations, such as:

- Tech Soup – (www.techsoup.org) provides drastically discounted software
- Google Apps – (apps.google.com) provides free Gmail, google cloud, and G Suite apps
- Microsoft Volume Discount – (https://www.microsoft.com/Licensing/servicecenter/Home.aspx) for discounts on Office365 and other Microsoft applications
- Microsoft – (https://portal.office.com/AdminPortal) Admin portal for Office365

Office Suite:

MX mainly utilizes standard Microsoft Office software for both Mac and PC. From the Office suite the main usage is from Word, Excel, PowerPoint (for worship and class slides), and Publisher (for the bulletins).

Bookkeeping:

MX has long relied on ***QuickBooks*** (https://quickbooks.intuit.com/) to manage the bookkeeping for the church. QuickBooks is also use for payroll processing. This application is loaded only on the computer utilized by the MX Bookkeeper (Elizabeth McPherson). Data is routinely backed up on a network storage device in the locked computer closet. The data is also encrypted and password protected.

Currently we are using a local version of the application loaded on our MX computer, however, we are investigating the cloud SaaS version. An issue exists with payroll that prevents us from migrating to the cloud at the moment.

Donations/Tithes:

Servant Keeper (https://www.servantpc.com/) is software specifically developed for religious institutions to track donations. All individual donations received by the church (via mail, direct deposit, weekly contribution, or on-line donations) are entered into Servant Keeper. This assists with annual tax donation letter preparation. Like QuickBooks, the data is backed up routinely to the network storage device in the locked computer closet, and is also encrypted and password protected. This application is loaded only on the computer utilized by the MX Bookkeeper (Elizabeth McPherson).

Currently we are using a local version of the application loaded on our MX computer, however, we are investigating the cloud SaaS version.

Bulletins:

Microsoft Publisher is used to create the weekly bulletin. These are stored on the hard drive of the MX secretary (Dolores Miller), and backed up the network storage device in the locked computer closet.

Worship:

Various software is utilized for the media used for Sunday morning worship and classes. Software is used for display of PowerPoint to congregation, recording of sermon audio and video, etc. All of this is important to the MX church but is beyond the scope of this document.

Antivirus:

The Windows computers in use at MX all run Windows Defender. The following review is from Wikipedia (https://en.wikipedia.org/wiki/Windows_Defender#Reviews):

> *During the December 2017 test of various anti-malware software carried out by AV-TEST on Windows 10 platform, Windows Defender has earned 6 out of 6 points in detection rate of various malware samples, earning its "AV-TEST Certified" seal.[32] Also, during February 2018 "Real-World Protection Test" performed by AV-Comparatives, Windows Defender has achieved 100% detection rate of malicious URL samples, along with 3 false positive results.[33]*
> *AV-TEST test of Defender October 2019 shows it provides excellent protection both against viruses and 0-day / malware attacks.*

Data

Per discussions with ministers and staff the following are the types of data maintained on church systems: Counselling notes, minutes from shepherding meetings, performance reviews, job offers, financial files, spreadsheets, directory information, bank account information, donation information, bulletin templates, building and facilities information, and other similar files.

Presently there is no standard storage location, backup schedule, or policy guidance on data classification (what is considered sensitive data).

Security Cameras

When theft, injuries, and other incidents occur at ministries, surveillance camera footage can help provide an account of what happened. Security cameras can even deter crime.

Some good thoughts and guidance from Brotherhood Mutual at **Exhibit G**.

At MX we utilize two different security systems: Google Nest, and Wyze. By policy, video footage will only be released at the approval of the Administrative Elders, even to law enforcement.

Google Nest:

These cameras offer hi-definition video saved 24/7 to the cloud. These have the most storage history and best resolution of the cameras used at the building. Because of the resolution these cameras use a significant amount of internet bandwidth to continuously upload video to the cloud. They are located in the following public areas:

1) foyer facing south doors,
2) hallway facing north doors,
3) 3rd floor children's classrooms (Sow-n-Grow area) facing doors,
4) 3rd floor facing doors, and
5) outside facing the main parking area.

As mentioned above, we have 24/7 monitoring of all doors to the MC building as well as to the children's area.

WYZE:

These are budget friendly cameras used to augment the video coverage of the main Nest cameras discussed above. These cameras record 7 days of video to a memory card on the camera. They also record 10-second clips of any movement noted to the cloud. These cameras are located in the following public areas:

1) MX office (no audio is recorded),
2) MX foyer facing auditorium door,
3) auditorium balcony facing down towards the stage,
4) auditorium stage facing main doors, and
5) 4th floor multi-use area.
6) Gym floor (recommended by insurance)
7) Gym door to outside

Internet of Things (IoT) Devices

MX has implemented several IoT devices. We use WEMO switches to allow automation of the parking lot lights. We use Nest Thermostats to automate and monitor temperature in 4th floor classroom and 3rd floor main Sow-n-Grow area. We use Nest Protect fire and smoke alarms in the 3rd and 4th floor area of the old building where the upgraded fire system did not reach. We also have a Ring doorbell at the south doors that notifies the office (with audio and video) of visitors.

Video Intercom

The secretary desk in the MX office has a video intercom unit connected to a camera at the main north doors. The unit allows the north doors to remain locked with visitors able to push a button to start a two-way conversation with the MX office. If visitor request to access building deemed appropriate the MX office can then buzz open the door. This provides additional safety for the MX office staff while maintaining safe guest access to the church staff.

- AIPHONE VIDEO INTERCOM (Model# JOS-1VW)
- KEYPAD (model# AC-10S)

Church Website, Communication and Scheduling

Website: www.McKnightCrossings.org redirected to https://www.mxchurch.org/ . We use Church Plant Media to host the website.
Currently, Brian Hill uploads the sermon file to Google Drive, and Dolores Miller loads it to our website. Brian Hill also loads video of the sermon to Youtube (channel https://www.youtube.com/channel/UCOkXSisXPAMDK-eCfU5STaA). Our website presents a limited threat vector.

Scheduling Software: Planning Center Services
Check-In Software: Planning Center Check-Ins
Current Streaming Software for kid's ministry: Be.Live
Live Streaming of services: During the COViD quarantine Sunday worship has been live-streamed via Facebook Live (some good discussion here … https://www.wowza.com/blog/facebook-live-for-churches)

III. DISCUSSION on RISK

Risk discussion at **Exhibit B** is from an IT textbook outlining basic risk concepts. This is important information as it lays out the guidance that risk tolerance is set by leadership, with the exception of laws outlining required controls for specific areas like HIPAA for specific individual health documentation and personal identifiable information (PII) such as bank account and social security information.

What this means is risk appetite is subjective, based on the amount of risk leadership is willing to accept. Also, risk and security should be considered by item or incident without consideration of medium. For example, if the church accepts the risk of having printed directories available to anyone in the public foyer of the building it should not expect any additional security of the same directory is digital. It would be inconsistent to expect one version of the directory (print) to require limited security and another (electronic) to require passwords, limited access, and audit logging. This is just a single example but the principle should hold for all church assets.

This is the most important section of this report. There is no "appropriate" security or level of risk, it is all dependent on the risk appetite of leadership. However, this does not apply where there are legal mandates, such as data privacy laws regarding: HIPAA, personally identifiable information (PII), SSN data security, Children's Online Privacy Protection Act of 1998 (COPPA), etc.

Note: MX does not receive any payment directly by credit card or store credit card information so is exempt from Payment Card Industry Data Security Standard (PCI DSS). This risk is mitigated by using PayPal.

IV. RECOMMENDED ENHANCEMENTS

1. Classify Data and Determine what is "Sensitive"

A data classification policy maps out a variety of components in an organization. It then considers every type of data belonging to the organization and subsequently classifies the data according to storage and permission rights. These data may perhaps be categorized as sensitive, public, confidential, or personal. A data classification policy should also take into consideration any specific data classification levels or categories adopted by industry regulations or standards. Data classification policies enable organizations to apply the appropriate level of security to data, lowering the company's overall risk.

BENEFITS OF DATA CLASSIFICATION POLICIES

- Data classification policies help an organization to understand what data may be used, its availability, where it's located, what access, integrity, and security levels are required, and whether or not the current handling and processing implementations comply with current laws and regulations.

- It is the most effective and efficient system for protecting data as it helps to categorize data to protect critical, sensitive, and classified information. If sensitive data get into the wrong hands, organizations may be liable for penalties for violating laws and regulations and they may suffer from financial loss or reputation damage.

- Data classification policies help organizations meet regulatory compliance as well as industry best practices and customer expectations.

- It also helps in optimizing designated security funds by allowing organizations to determine what security measures to invest in based on the amount of sensitive data that requires protection, where it's located, and the threat landscape.

Example of Data Classifications:

A. Restricted Data

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the Church or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to restricted data.

For MX, primary focus should be placed on identifying and securing data that should be restricted.

B. Private Data
Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the Church or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

C. Public Data
Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the Church and its affiliates. Examples of Public data include sermons, and information already made public on our exterior facing website. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

2. Employee Security Training

Employees are part of an organization's attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. It is recommended that employees receive periodic training in the following areas:

- Phishing: Employees should be educated on how to spot and report phishing and the dangers of interacting with suspicious links or entering credentials on a spoofed page. Overviews should cover spear phishing, suspicious phone calls, contact from suspicious social media accounts, etc.

- Physical security: Physical security requirements can vary on an organization's nature. Since businesses should already have a physical security policy in place, this is a great opportunity to make sure employees understand the parts of the policy that apply to them, such as locking desk drawers and rules about allowing guests into the office. Training should also review how to report physical security risks, such as someone in the building who isn't wearing a guest badge or sensitive data that is left exposed.

- Desktop security: Outline the potential consequences of failing to lock or shut off computers at appropriate times and plugging unauthorized devices into workstations.

- Wireless networks: Explain the nature of wireless networks and outline the risks of connecting to unfamiliar ones.

- Password security: Complex password requirements and prompting employees to change their passwords on a regular basis should already be enforced, but password security training is still important to explain the risks involved in reusing passwords, using easy-to-guess passwords, and failing to change default passwords immediately.

- Malware: A training session on malware should define the types of malware and explain what they are capable of. Users can learn how to spot malware and what to do if they suspect their device has been infected.

3. Adopt a Security and Acceptable use Policy (AUP)

The acceptable use policy protects MX from many legal actions, while clearly communicating to employees your expectations regarding their behavior. It is far better to lay out acceptable usage and get employees on board early than to have to backpedal if something goes wrong.

An example Acceptable Use Policy (AUP) is attached at **Exhibit J**.

4. Backup and Secure Data

By performing frequent data backups, you can save your ministry from losses that can be costly in terms of time, effort, money, and even privacy. These days, data backups are increasingly important because ministries store more digital files than ever. Fortunately, because of increasing backup options and decreasing costs, establishing a backup system is easier than ever.

When forming a plan for backing up data, it's important to decide which files are critical to ministry operations and which ones are less important. If a natural disaster destroyed all the ministry's computers, which files would you need to restore first in order to get ministry operations back to normal? These should be first on the list of files to back up—files related to accounting, payroll, worship services, and other critical functions.

It also helps to know where ministry employees save critical files. Are the files located on employee computers' hard drives or a networked server? Do employees use laptops or desktop computers? Do they keep ministry data on their mobile devices? Centralizing the most important files in a handful of folders (for example, the My Documents folder or a file server) can make the backup process easier.

V. EXHIBITS

Exhibit A – org chart

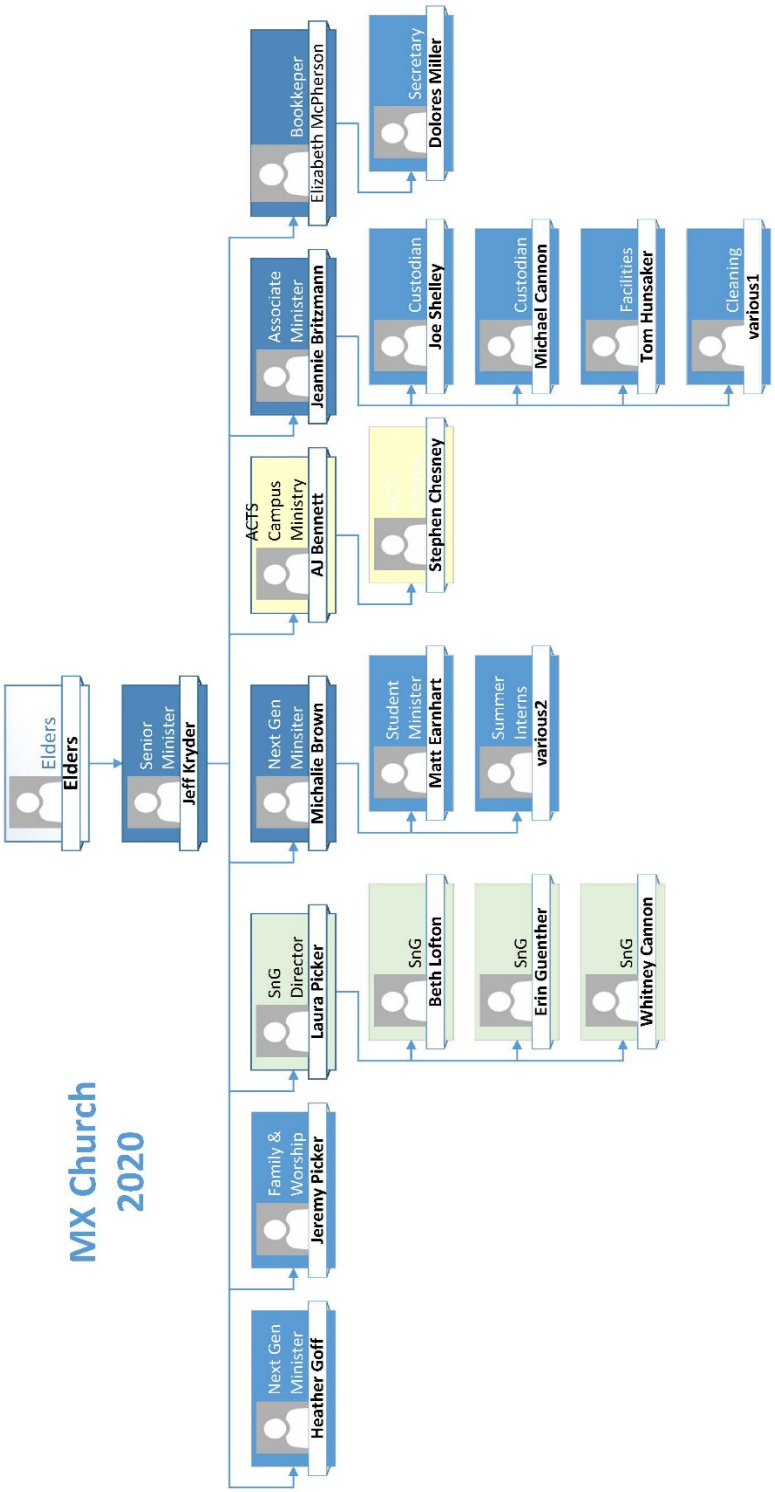

Exhibit B – Risk Concepts

Below text in blue is from an IT textbook outlining basic risk concepts.

Risk appetite is the level, amount, or type of risk that the organization finds acceptable. This varies widely from organization to organization, based on factors both internal and external, and can change over time.

Risk fundamentals:

- Risk is the likelihood an impact will be realized
- Risk can be reduced but never eliminated
- Organizations accept a level of risk that allows operations to continue in a successful manner
- It is legal and defensible to accept risks higher than the norm, or greater than your competitor, except risks to health and safety, these risks must be addressed to the industry standard or whatever regulatory motif to which your organization adheres.

An organization cannot accept risks to health and human safety that are beyond industry standards and known best practices; to do so would be unethical, and it would expose the organization to a great deal of liability (which creates its own risk, which also must be considered). However, individuals can accept such risks on their own behalf. For instance, commercial fishing has consistently been among the professions with the highest fatality rates in the United States for the past 100 years (in terms of number of hours worked per death), yet there is no shortage of people willing to engage in that industry. For the individual workers, the level of risk is both known and acceptable. From an organization's perspective, however, the relatively high possibility of fatal accidents does not obviate the need for ensuring adherence to industry best practices (perhaps life vests, tether lines, and so forth), and does not remove liability.

Risk is involved in every activity. We can manage risk, attenuate it, even mitigate it, but there is always an element of risk in operations. When we chose to mitigate risk by applying counter, measures and controls, the remaining, leftover risk is called residual risk. The task of the security program is to reduce risk until it falls within the acceptable level of risk according to the organization's risk appetite.

The risk appetite of an organization is set by senior management, and is the guide for all risk-management activities in the organization.

All organizations must constantly evaluate risks to all systems, applications, and data, coupled with management's appetite for risk and the level of risk they are willing to accept. Although it is not possible to totally eliminate all risks, a sound approach is to mitigate those risks you can, and to minimize the likelihood of occurrence of the rest and any damage they could cause. Many decisions in risk management are also guided by specific requirements from regulatory or legal systems, as well as potential and specific penalties for data access or exposure as a result of a successful exploit.

Exhibit C – Ministry Data Security

Protect Ministry Data and Computers

(from Brotherhood Mutual)

Safeguarding information can help deter theft, preserve privacy, and avoid lawsuits

Churches commonly collect and store members' personal information. Everything from mailing lists and donation records to Social Security numbers and payment card information may be kept in the average church database or filing cabinet. Unsecured, this data could make church members vulnerable to thieves—putting ministries and church members at risk. Carefully protecting data not only makes business sense, but it also can reduce the likelihood of crippling data loss, embarrassing public disclosures, and lawsuits.

Physical Security

Physical security is a vital aspect of data protection. The Better Business Bureau offers these data safety tips for small businesses:

1. Shred papers containing personally identifiable information before throwing them away.
2. Send and receive business mail from a secured mailbox or post office box.
3. Verify a church member's identity before providing any personal or financial information by telephone or email.
4. Secure your building with locks and alarms.
5. Store business, employee, and membership records in locked cabinets.
6. Limit staff and volunteer access to sensitive information.
7. Train office workers how to protect the privacy, confidentiality, and security of personal information.

Computer Security

Data housed on computers is particularly vulnerable to theft—especially when computers are connected to the Internet. One errant click can leave an entire congregation open to identity theft. Because hackers go to great lengths to ensure that you can't easily shake them off, the best medicine is prevention. Here's what you can do:

1. **Limit access with passwords.** Use passwords to limit employee and volunteer access to sensitive information. Train office workers to keep passwords private. Be sure to issue new passwords when an employee or volunteer stops working in the office and no longer needs to view ministry records.
2. **Keep software up to date.** Windows and Mac computers can be set to automatically apply security updates. Many of the individual programs and apps on your computer can also be set to automatically apply updates. Taking the time to enable the automatic settings now will ensure you don't forget when you are busy later.
3. **Install a dependable firewall.** Both hardware and software firewalls are designed to prevent unauthorized access to a network.
4. **Secure your wireless network.** If your church uses Wi-Fi for staff members and you would like to offer Wi-Fi Internet access to the congregation or visitors, make sure to set up an additional and separate guest network that only has access to the Internet. Wi-Fi networks should always be password-protected. The password for the guest network can be shared each week via the church bulletin, slides, signs or other method. As with all passwords, they should be changed regularly. For more information, read *Protect Computer Networks When Offering Free Wi-Fi*.
5. **Keep up with anti-virus software updates.** Anti-virus software can prevent or reduce the impact of virus infections. Paid anti-virus software generally keeps itself up to date as long as you pay your subscription fee each year. Check periodically to ensure the license period hasn't expired. Some free anti-virus software is available—check the licensing terms to make sure that the free use includes use in a church or non-profit entity.
6. **Fine-tune your browser settings.** Adjust your browser to use a higher security setting. Most browsers can automatically check for security updates and install the newest version.
7. **Scan computers weekly for malicious software.** Most virus and spyware protection software can be programmed to do this automatically.
8. **Preserve critical data.** Back up business records daily, weekly, or monthly, depending on how often data is edited and your tolerance for risk of losing the data. Store backups in a secure, off-site location, such as a safe deposit box. This protects your ministry from losing records to computer breaches and other events, such as tornadoes, floods, or fires.
9. **Know what you're installing.** Ask yourself, "Do I know and trust the source of this software?" Reputable software publishers will either avoid including adware/spyware with their products or clearly tell you how to download the software without the "extras."

10. **Protect your website.** It's best to host your ministry website—and online giving platforms—with a trusted vendor that uses industry-standard security measures. Be sure to thoroughly screen the vendor and review any contract before signing it.

Beware of Scams

Scammers are finding more ways to entice people into giving up personal and organization data. From sending emails pretending to be the pastor or other ministry leader asking for money to be wired immediately to sending emails demanding W-2 files be sent via PDF format, scammers are targeting nonprofit organizations. Take steps to protect your ministry:

1. **Watch what you click.** Though it can be time-consuming to read pop-up messages, it's important you know what you're doing before you click. Many fraudsters are counting on you to be in the habit of simply clicking on links or selecting "OK" or "Yes" on everything you see. When in doubt, avoid clicking the link. Instead, call the company or visit its website, using contact information you already know to be genuine. Do not enter usernames or passwords if you don't know why you are being asked for them.
2. **Never send personal information through email.** Avoid sending personal information through email. Before submitting financial information on a website, look for the "lock" icon, often located in the browser's address bar. This icon indicates that your information will be transmitted securely.
3. **Monitor financial accounts.** Review credit card and bank accounts online for unauthorized charges. Call your credit card company or bank immediately if you notice unauthorized charges.
4. **Report scams.** Report suspicious activity to the Federal Trade Commission (FTC) via their website, ftc.gov. If you receive spam email that asks you to supply sensitive information, forward it to spam@uce.gov. Visit the FTC's website to learn other ways to avoid email scams and deal with deceptive spam.

If your ministry's data is hacked, contact law enforcement immediately. This is especially critical if financial information has been compromised. Notify your insurance agent or insurance company's claims department, as well.

Exhibit D – Cyber Security Checklist

Below from Brotherhood Mutual - https://www.brotherhoodmutual.com/resources/safety-library/risk-management-forms/cyber-security-checklist/

Cyber Security Checklist	YES	Note
1. Do you perform monthly backups of business and financial information and store it in a secure, off-site location, such as a safe deposit box or a reputable cloud-based storage service?	X	
2. Do you have policies in place to protect confidential information like contribution records, counseling notes, and other sensitive information?		A
3. Do you have policies in place to report a data breach in accordance with state law and to protect your ministry from legal action?		B
4. Do you have policies in place to maintain compliance with Payment Card Industry (PCI) rules for use, processing, and storage of credit card information?		C
5. Do you appoint a senior staff member who has responsibility to ensure security policies are in place and followed?		
6. Do you limit access to sensitive data and systems to authorized individuals and is that data password protected and/or encrypted?	X	
7. Do you change passwords for user accounts and cloud services on a regular basis and when an employee leaves?	X	
8. Do you enforce or encourage the use of two-factor authentication for access to email, church records, and other sensitive data?		D
10. Do you work with a qualified staff member or computer support company to secure your computer systems?	X	
11. Do you update your operating system for security reasons?	X	
12. Do you update virus and spyware protection on systems, devices, and applications?	X	
13. Have you installed firewalls that are designed to prevent unauthorized access to your computer network?	X	
14. If you offer wireless internet access to your attendees, have you created a separate, private network for the church's administrative computers?	X	
15. Do you protect against objectionable or illegal WiFi use by blocking questionable websites, password-protecting the wireless network, and asking users to agree to an Internet Usage Policy?		E

Response to Questionnaire Above:

A – See Recommendation #1
B/C – At present no PCI or related data collected
D – Two-factor authentication is required for the key admin accounts, such as Google Apps, Microsoft Admin Portal, and access to the security cameras.
E –MX-guest wifi has a splash page with usage guidance. Recommend updated the Acceptable use policy (AUP).

Exhibit E – Cybersecurity Tips for Churches

Cybersecurity Tips for Churches

1. *Perform regular security assessments and checks.*
2. *Provide ongoing employee security training and testing.*
3. *Implement enforced security policies, password policies, Multi-factor Authentication, and mobile device security.*
4. *Implement a robust Business Continuity plan and infrastructure.*
5. *Utilize Unified Threat Management (UTM) Firewalls and Secure Wi-Fi.*
6. *Utilize and implement Disk Encryption.*
7. *Be diligent about patching.*

Exhibit F.1 – iNet Scan : MX-main

Below are the results of a network scan performed May 31, 2020 on the ***MX-main*** network. Items marked as "unknown" below are those where the scanning tool could not clearly identify the hardware detected, and is not inherently an item of concern.

iNet Scan - May 31, 2020

#name	#ip	#modelIdentifier	#modelDetail
02aa01ac451305vu	192.168.1.78		
192.168.1.13	192.168.1.13	Printer	HP Color LaserJet 4700 [2725F2]
5268ac	192.168.1.67		
amazon-8d21387ab	192.168.1.119		
Canon70Ca94	192.168.1.132	Printer	Canon MF420 Series
Dell 06Pd2Ml	192.168.1.128		
Desktop Laf35Sk	192.168.1.104		
homeportal	192.168.1.254		
Hp071390	192.168.1.173	Printer	HP Color LaserJet Pro M478f-9f [071390] (7)
kmb7ec9d	192.168.1.127	Printer	Kyocera CS 3051ci
mBret -7086	192.168.1.168	iPhone10,4	13th Gen. (Late 2017)
mr18-foyer-00180ad20cc0	192.168.1.114		
mr34-4thfloor-00180aa82f70	192.168.1.112		
mr34-office-881544446e50	192.168.1.111		
Mx Frontoffice	192.168.1.75		
mx-office	192.168.1.82		
mxs-mac-mini	192.168.1.156		
mxs-mac-mini	192.168.1.158		
s-mr18-00180ae80d60	192.168.1.113		
sip-t21p_e2	192.168.1.125		
unknown2caa8e1b61b6	192.168.1.105		
unknown2caa8e096d96	192.168.1.154		
unknown2caa8e208df0	192.168.1.179		
unknown2caa8e060378	192.168.1.150		
unknown18b430d7ad85	192.168.1.116		
unknown90e2021ef837	192.168.1.172		
unknowna4da222c57ad	192.168.1.91		
unknowna4da222c5163	192.168.1.87		
unknowna4da22316ae8	192.168.1.120		
unknowna4da22316bfc	192.168.1.123		
unknownd4f0b401ccc4	192.168.1.110		
w60b	192.168.1.146		
Wdmycloud Mx	192.168.1.98		
Wdmycloudmirror	192.168.1.203		
wemo	192.168.1.65		
wemo	192.168.1.69		
wemo	192.168.1.70		
wemo	192.168.1.72		
wemo	192.168.1.108		

Exhibit F.2 – fing Scan : MX-main

Below are the results of a network scan performed May 31, 2020 on the ***MX-main*** network

FiNG : 31-May-20 MX-Main network

Address	Hardware address	Name	Make	Model	Hostname	Type	State	First seen
192.168.1.13		NPI2725F2	HP	HP Color LaserJet 4700		Printer	UP	5/31/20, 12:03:26 PM
192.168.1.65		MX-PrkLight-S3 Farthest	Belkin	LightSwitch	wemo	Light	UP	5/31/20, 12:03:26 PM
192.168.1.67		5268ac			5268ac	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.69		MX-PrkLight-S1 Closest	Belkin	LightSwitch	wemo	Light	UP	5/31/20, 12:03:26 PM
192.168.1.70		wemo			wemo	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.72		MX-PrkLight-S2 Center	Belkin	LightSwitch	wemo	Light	UP	5/31/20, 12:03:26 PM
192.168.1.75	F8:0F:41:D5:6C:76	MX-FRONTOFFICE:			mx-frontoffice	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.78		02aa01ac451305vu			02aa01ac451305vu	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.82	30:10:B3:B8:18:24	MX-OFFICE: eMcPherson:			mx-office	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.87		unknowna4da222c5163			unknowna4da222c5163	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.91		unknowna4da222c57ad			unknowna4da222c57ad	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.98		WDMyCloud-MX	Western Digital	WDMyCloud	wdmycloud-mx	NAS	UP	5/31/20, 12:03:26 PM
192.168.1.104	80:CE:62:F2:AE:F6	DESKTOP-LAF35SK	HP		desktop-laf35sk	Computer	UP	5/31/20, 12:03:26 PM
192.168.1.105		unknown2caa8e1b61b6			unknown2caa8e1b61b6	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.108		3rd Floor East Doors	Belkin	LightSwitch	wemo	Light	UP	5/31/20, 12:03:26 PM
192.168.1.110		unknownd4f0b401ccc4			unknownd4f0b401ccc4	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.111		mr34-office-881544446e50			mr34-office-881544446e50	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.112		mr34-4thfloor-00180aa82f70			mr34-4thfloor-00180aa82f70	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.113		s-mr18-00180ae80d60			s-mr18-00180ae80d60	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.114		mr18-foyer-00180ad20cc0			mr18-foyer-00180ad20cc0	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.116		unknown18b430d7ad85			unknown18b430d7ad85	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.119		Jeremy's Fire TV	Amazon	Fire TV	amazon-8d21387ab	Media Player	UP	5/31/20, 12:03:26 PM
192.168.1.120		unknowna4da22316ae8			unknowna4da22316ae8	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.123		unknowna4da22316bfc			unknowna4da22316bfc	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.125		sip-t21p_e2	Kyocera	F-Series	sip-t21p_e2	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.127		KMB7EC9D			kmb7ec9d	Printer	UP	5/31/20, 12:03:26 PM
192.168.1.128	D8:12:65:90:D2:45	DELL-06PD2ML			dell-06pd2ml	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.132	A0:C9:A0:32:4B:9A	MF420 Series	Canon	MF420 Series	canon70ca94-2	Printer	UP	5/31/20, 12:03:26 PM
192.168.1.146		w60b			w60b	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.150		unknown2caa8e060378			unknown2caa8e060378	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.154		unknown2caa8e096d96			unknown2caa8e096d96	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.156		mxs-mac-mini	Apple	Mac mini (2007)	mxs-mac-mini	Desktop	UP	5/31/20, 12:03:26 PM
192.168.1.158		mxs-mac-mini	Apple	Mac mini (2007)	mxs-mac-mini	Desktop	UP	5/31/20, 12:03:26 PM
192.168.1.161		09aa01ac45180qb8			09aa01ac45180qb8	Generic	DOWN	5/31/20, 12:03:26 PM
192.168.1.168		mBret -7086			mBret -7086	Generic	UP	5/31/20, 12:03:24 PM
192.168.1.172		unknown90e2021ef837			unknown90e2021ef837	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.173		HP9C7BEF071390	HP		hp071390	Printer	UP	5/31/20, 12:03:26 PM
192.168.1.179		unknown2caa8e208df0			unknown2caa8e208df0	Generic	UP	5/31/20, 12:03:26 PM
192.168.1.203		WDMyCloudMirror	Western Digital	WDMyCloudMirror	unknown0090a9e7fbf4	NAS	UP	5/31/20, 12:03:26 PM
192.168.1.254		homeportal			homeportal	Generic	UP	5/31/20, 12:03:26 PM

Exhibit G – Benefits of Surveillance Cameras

From Brotherhood Mutual

Benefits of Surveillance Cameras:

1. Reduce the potential for crime
Criminals often look for less secure facilities, or facilities that offer the least chance of being caught. They'll typically avoid buildings with alarm systems or surveillance cameras. In one study, security cameras were found to be an effective deterrent to burglary. Security cameras may also deter other criminal acts.

2. Resolve disputes
Video surveillance can provide an account of what happened if there is a dispute about a situation. Did someone ignore caution tape and trip over a construction hazard? Did a youth volunteer have inappropriate contact with a child in a classroom? When you can go back and review video footage, it enables ministries to have an additional layer of protection against false claims or allegations.

3. Capture criminal activity
Depending on the type of camera and its placement, you may be able to identify the person(s) responsible for a crime. Most cameras will at least show what happened, enabling you to provide a general description of the perpetrator(s) and any associated vehicle.

4. Provide remote access
Being able to see inside your building is helpful, especially when an alarm is triggered in the middle of the night. If ministry leaders can quickly see inside and outside the building, they'll be able to provide useful information to responding law enforcement. And if there is someone breaking into the church, they can notify the police, who can make the call a priority. This also provides peace of mind for whoever responds to the alarm, letting them know if it's just the wind that opened an unlocked door or if someone has smashed through the front doors.

Balance Security with Privacy

Aside from the benefits of surveillance cameras, your efforts should balance ministry security with individual privacy. Think about the following issues before pressing the "record" button:

Notification. It's a good idea to post signs announcing that surveillance cameras are in use. Even when not required by law, a notice sign near the property line or building entrance can improve the deterrent effect of cameras.

Privacy. Placing cameras in public places—such as the auditorium, a foyer, classrooms, or hallways—where an individual can expect to be seen by others – is generally acceptable. However, restrooms, locker rooms, and other private spaces should be off-limits for cameras.

Exhibit H - Resources

Resources

- Nonprofit guidelines for cybersecurity and privacy (Microsoft)
- What nonprofits need to know about security: A practical guide to managing risk (Idealware)
- 7 Ways Cloud Computing Propels IT Security (TechImpact)
- How Nonprofits Can Ensure Security and Compliance of Sensitive Data in the Cloud (NTEN)
- Cyber Security Q&A: Nonprofits at Risk (Third Sector Today)
- Feeling insecure about security? Protecting your nonprofit's data is not rocket science (National Council of Nonprofits)
- Top Ten Cybersecurity Tips for Nonprofits: Managing your technical and legal risks (Venable, LLP)
- Seven Deadly Weaknesses of Nonprofit Security (And How to Address Them), NTEN
- Protect Ministry Data and Computers
- You can help protect your organization using the information at FTC.gov/Cybersecurity.

Exhibit I – Video Youth Group Meetings

From ... https://ministrytoyouth.com/zoom-youth-group-dos-donts-and-alternatives/

ZOOM YOUTH GROUP: DO'S, DON'TS AND ALTERNATIVES

With many youth groups meeting on Zoom or other video platforms, we put together a list of do's, don'ts and alternatives.

This list was comprised on youth leaders like you, in the trenches, learning as they go what works and what doesn't.

Nick Diliberto, Ministry to Youth

The #1 choice right now seems to be Zoom, so let's start there.

What is Zoom?

Zoom meetings have quickly become a helpful ministry tool. Since churches are unable to meet in person, this platform allows leaders to connect face-to-face with those in their church for little to no cost.

Zoom is a video conferencing/web conferencing platform. Anyone can easily set up an event with one "host" and invite others to participate.

Their Basic Plan gives you the ability to hold unlimited meetings for free, as long as you would like. You are limited to 40-minute meetings when you have three or more participants.

The Pro Plan is $14.99/month and enables you to have up to 100 participants and up to a 24-hour meeting time limit. It also includes cloud space to store files, recordings, and videos.

How does it work?

You can host a Zoom meeting in only a few steps:

1. Select your Zoom plan.
2. Choose "Host a Meeting" or "Schedule a Meeting."
3. You can start with or without video.
4. Next, invite participants to the meeting.
5. Give your meeting a title and description.
6. Choose the time when the meeting will begin.
7. Set-up a password for participants to enter that will enable them to join the meeting.
8. Host your meeting.

One feature that is convenient for those who are hosting small groups, is the option of having "Breakout groups." This allows you to have multiple small groups happening at one time through one paid account.

Here are a few do's and don'ts from fellow youth ministry leaders to make your Zoom meetings awesome…

Do's

- Create a "waiting room" that allows students to gather in one place and ensure that only those who have been invited will be participating in the meeting.
- Keep students engaged by asking them to lead specific segments of your meeting – lead prayer, read Scripture, and even keep score during a game.
- Help students to prepare and look forward to the meeting by sending the info ahead of time. This includes things like service order, Bible Study format, questions, etc.
- Maintain order. Because students have an extra reserve of energy and excitement to see each other, lay down a few ground rules that will keep everyone from talking over each other.
- Insert games into your meeting time. Platforms, such as Kahoot.com allow you to create trivia games and more that can be utilized during your meetings.
- Have a designated person that can chat with students during the Zoom call. These "co-hosts" can mute people, stop video, and chat with students during the meeting.

Don'ts

- Don't share your Zoom meeting ID and password publicly. Make this info available only to those who you invite to participate in the event.
- Don't assume that Zoom is completely secure. Some youth leaders have reported hackers that have shared inappropriate content during their Zoom meeting.
- Don't begin the meeting until everyone mutes their microphone. This will cut down on extra noise and conversation.

Here are two quick tips from Taylor Brown that you can use when you are teaching via video – either live or recorded.

THE EYE OF THE LENS IS THE EYE OF THE VIEWER
It's ok to look away. Constant direct eye contact is weird and creepy. Try to be as normal as you would in person, looking away, up in thought, down at notes, etc.

LESS VOLUME; MORE POWER
Low volume makes people lean in. You are speaking into someone's earbuds or speakers. Use the opportunity to speak softly, forcing them to really listen closely.
Pauses create weight. Don't rush through what you are teaching. Pause to allow them to think, reconnect, or even laugh.

Exhibit J – Acceptable Use Policy (AUP)

Technology Network/Internet Acceptable Use Policy

McKnight Crossings Church of Christ offers to staff server access for storage, cloud storage, email account, internet access, projector printers, copiers and other technological resources. These resources are intended for church and related church activities. These guidelines and conditions of use apply to all staff and members with access to these resources. Operation of the network relies upon the proper conduct of the end users who must follow these guidelines and conditions of use. The policy represents McKnight Crossings Church of Christ's good faith efforts to promote the safe, ethical, responsible, and legal use of the Internet, support the effective use of the Internet for outreach and communication purposes, and ensure accountability.

McKnight Crossings Church of Christ reserves the right to manage its technology system as it sees fit. The McKnight Crossings Church of Christ eldership will establish what inappropriate use is and this decision is final. The eldership has the right to revise this policy at any time and revisions will take effect immediately. The eldership retains the right to deny, revoke, or suspend specific user privileges, or restrict access to technology resources suspend, terminate if deemed necessary.

Computer, Network, and Internet Guidelines and Conditions of Use

Acceptable Use – Acceptable use is always ethical, reflects honesty, and shows courtesy. It demonstrates respect for intellectual property, ownership of information, and system security structures. Its use is to provide access to tools and resources to further the message of Christ and His Church.

Privileges/Consequences – The use of technology is a privilege. Users must recognize and practice acceptable, moral and lawful uses of the technology. Inappropriate use may result in a restriction of privileges, loss of privileges, suspension, loss of employment and/or other disciplinary action.

Privacy – Users have no privacy expectations in the contents of their files, emails and transfer of information and records of their activity while on or using file storage and church network. McKnight Crossings Church of Christ reserves the right to monitor, examine, restrict, or remove any material used, generated or stored by any user that is on its technology systems.

Filtering - McKnight Crossings Church of Christ filters access to inappropriate material to its best ability. Even with the best security and filtering, users may discover controversial or offensive information and materials, either accidentally or intentionally. McKnight Crossings Church of Christ does not excuse the use of controversial or offensive materials and cannot be

held responsible for such use. If such inappropriate or offensive material is inadvertently encountered, it shall be disengaged from immediately**.**

Data File Protection - Church related files are to be saved to the file server. Data files are backed up routinely to secure cloud storage. Files on server and backed up in the cloud are property of the McKnight Crossings Church of Christ. Staff members are encourage to practice personal backup procedures to insure recovery of lost data files for their personal non-church related files.

Email – A church email account is provide and is the property of McKnight Crossing Church of Christ. The church email is to be used for all communication regarding church business and related activities. Group emails are to be sent in groups of 50 or less; over 50 is considered spamming.

Personal Computer – Staff personal computers are provided access to McKnight Crossing's network. Staff are to keep their computer updates current and provide anti-virus on their computers (Windows). Peer to Peer and proxy websites are not to be used on the church network. Members are restricted from downloading files on MC CoC network.

PURPOSE: To define and describe McKnight Crossings Church of Christ's acceptable and unacceptable uses of provided technology and access to information resources.

1. McKnight Crossings Church of Christ's "Computer network" shall include services, hardware, software, the transfer of information from one point to another, emails, access and connection to the Internet, storage of information, data, or any system, network, or equipment attached to the computer network. McKnight Crossings Church of Christ has the right to place restrictions on use of the computer network.

2. McKnight Crossings Church of Christ will not be responsible for any damages users may suffer, including but not limited to, loss of data, interruption of service, or exposure to inappropriate material or people and financial obligations arising through the unauthorized use of the computer network.

4. Access to electronic information related to staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

5. Social technology is an important means of communication with members and the community. Staff members are required to represent and maintain respect, dignity and discretion. Staff actions are to demonstrate concern for the safety and protection of children and members in all interaction.

   With specific regard to social media, as a church employee, one must:

- Understand that staff are accountable for their postings and other electronic communications that are job-related, particularly online activities conducted with a church e-mail address, or while using church property, networks, or resources.

Recognize that:

- Social media activities may be visible to current, past, and prospective members and serving as a role model is a critical aspect of one's work at the church; and accordingly, one must exercise appropriate discretion when using social media (even for personal communications) when those communications can impact one's role at the church.

6. Attempts to compromise the security, reliability, or the functionality of any McKnight Crossings Church of Christ technology systems will be considered a violation of this policy. This includes, but is not limited to, the uploading or creation of computer viruses, deletion or alteration of other user files or applications, removing protection from technology tools, or the unauthorized blocking of access to information, applications, or areas of the network, or unauthorized access to outside proxies in order to receive blocked unauthorized services such as instant messaging, outside email, peer-to-peer functions (music & games), etc.
    - Installing using and playing peer-to-peer applications on church equipment is prohibited and personal computers are not to run these applications while in the building.

7. A few examples of user activities that violate this policy:
    a. Commercial advertising not related to church business or unethical/illegal solicitation.
    b. Accessing, creating sending or posting a file, message, web site that contains pornographic, obscene, racist, sexist, inflammatory, threatening or slanderous toward others pictures, videos, stories, or other material; making copies of such material, or distributing or exposing others to such material.
    c. Creating and or placing a computer virus on the network or any workstation.
    d. Revealing home addresses, e-mail addresses, or phone number of other staff, members or former members.
    e. Harassing others or requesting or distributing addresses, home phone numbers, or other personal information, which could then be used to make inappropriate calls or contacts.
    f. Sharing passwords. The only person to ever use a password is the person to whom it belongs.
    g. Any internet usage that would embarrass, discredit, or jeopardize the safety of any member or staff member.
    h. Using music players, games, toolbars or other application that use peer-to-peer technology.
    i. Any usage that violates local or federal laws.
    j. Failing to report violations of this plan or other conditions that may interfere with the appropriate and efficient use of church resources. Users are required to report any misuse of the Acceptable Use Policy to the McKnight Crossings Church of Christ eldership.

Faculty & Staff Technology Network/Internet

Permission Form and Acceptable Use Agreement

The signatures on this Technology Network/Internet Acceptable Use Agreement indicate the parties who have signed have read the terms and conditions carefully and understand their significance.

USER

I have read and understand **McKnight Crossings Church of Christ's Technology Network/Internet Acceptable Use Policy** and will abide by the stated procedures. I am aware that it is impossible for McKnight Crossings Church of Christ to restrict access to all controversial and offensive materials and I will not hold them responsible for materials acquired. I understand that a violation of this policy may result in the loss of computer privileges, suspension, termination or other disciplinary action.

Staff Name

User Name (please print): _____

Staff Signature

User Signature_____ Date_____