We understand the disruptive impact COVID-19 can have on your ministry. Empty buildings (including churches) are typically more susceptible to criminal activity and property damage. Consider these preparations should you choose to work and worship remotely:

- Make sure all employees and volunteers have emergency contact numbers for each other.
- Ensure your business protocols are shared with staff; share an organizational chart. Create one if it does not exist.
- Make sure your member roster is updated with contact information, including email addresses, to ensure continued connection with all who are part of the congregation.
- Put a hold or temporary forward on mail delivery so it doesn’t pile up outside of the church. Reach out to your providers to see if all bills can be moved to electronic notification.
- Make sure all garbage is removed from inside and outside of the building.
- Conduct a thorough walk-through of your entire facility. Take photos and notes of current condition of the building. Make sure all heating vents and furnaces are kept clear of any debris such as clothing, paper products, etc.
- Make sure all windows are locked and secured, systems are safely shut down, and all unnecessary appliances are unplugged.
- If you have a security monitoring service, contact them to let them know your plans. If you do not have one, consider installing an alarm system. Alarms will deter individuals from attempting to enter the building and can quickly alert authorities when necessary.
- If you cannot install an alarm system at this time, consider contracting with a security company to patrol the property. Security services can be contracted to have Patrol Guards check your facility at random times. These guards are a great way to deter crime and can provide quick notification if there are any concerns.
- Consider motion-activated lights and general lighting which can help protect vacant buildings. Keeping entryways and other areas around the building well-lit will deter individuals from attempting to enter the building.
- Make sure to keep your thermostat set at an appropriate range. During these colder months, keep the temperature set at a minimum of 55 degrees in order to prevent pipes from freezing.
- Drive by the location several times a week to complete an exterior inspection. Vary the times/days so there is no set pattern.
- Think through transfer of authority if leadership is at risk of quarantine or has health restrictions. More than one person should be aware of the chain of command, so please share it with a few trusted sources.
- You should currently have two signers, but should one of those signers be unavailable for an extended amount of time, you should have a third identified to help pay bills and payroll.
- If your pastor becomes ill, notify your judicatory office.
- Investigate on-line giving options.
- Identify which operations are critical to survival and recovery: Include payroll, expedited financial decision-making, and accounting systems to track and document costs.
- Stored documents should be scanned and uploaded to the cloud (securely) if they are not already: insurance documents, church by-laws, personnel documents, leases, deeds, contracts, etc. If you do not or cannot store in the cloud, take documents with you.
- Other considerations for working remotely and IT concerns in a remote working world are on page 2.
Working Remotely and IT Considerations

Some states have issued Lockdown or Shelter in Place Orders. Regardless of the specific phrase, the meaning is the same: do not go out unless it is necessary. The primary purpose for these orders is to reduce the spread, or “flatten the curve” of COVID-19. According to the CDC, limiting our contact with others is critical in order to achieve this outcome.

As many companies and people move to a remote working environment, there are many things to consider! Make sure to check in with staff often via phone or virtual options. Loneliness can set in quickly.

Advice for IT and Network Administrators working from home.

- Make sure all devices and systems are encrypted. It is a high risk when devices leave the premises, they are often lost or stolen. Make sure all devices and systems are fully updated. Updates and patching are key to your protection.
- Make sure you have a secure connection to your organization’s network such as VPN (Virtual Private Network) with MFA/OTP (Multi-factor Authentication/One-Time Passwords). VPN is one of the best tools if configured correctly. Ensure MFA or OTP on all VPN connections to increase security. Make sure you enable MFA/OTP for all secure cloud apps including your email systems to help prevent common cyberattacks.
- Make sure your devices are fully protected with web filtering and antivirus software specifically designed to detect malware and prevent computer infections, as well as clean computers that have already been infected.
- If you are using Cloud storage, make sure users are using the organization’s storage. We often find users are using their personal cloud storage to store/share data. Organizations won’t be able to protect and secure that data.
- Make sure users are only using approved applications and services.
- Make sure you have good back up. Follow the 3-2-1 plan. The US-CERT (United States Computer Emergency Readiness Team) recommends you should have 3 copies, 2 media types, 1 offline or offsite copy.

- Make sure you are tracking “church inventory” as staff take items home.
- Test remote access capabilities before you are forced to close.
- Encourage staff to: designate “office” space. Create a quiet place to concentrate and spread out.
- Find an area in which work-related material can be stored and organized and secured.
- Adhere to the same work schedule that is followed in the office. If it is not possible to adhere to your schedule, alternatives should be discussed with and approved by your supervisor.
- Plan to be available via phone, email and whatever means your ministry uses.
- Anticipate interruptions and manage outside demands. Establish rules or guidelines for yourself and others to make it clear that you are engaged in your job/work and not available for non-essential issues.
- Remind staff: Cybercriminals are opportunistic, the pandemic may be used to perpetrate phishing schemes. Let staff know about these dangers and the need to verify the source of a communication before clicking on links or attachments.