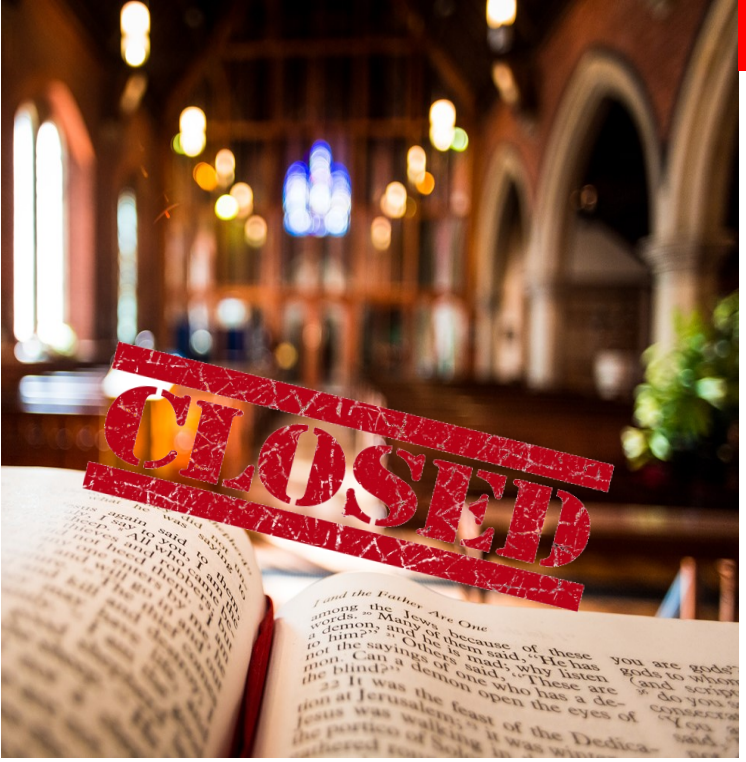

Working Remotely and IT Considerations

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.

- 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.

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.