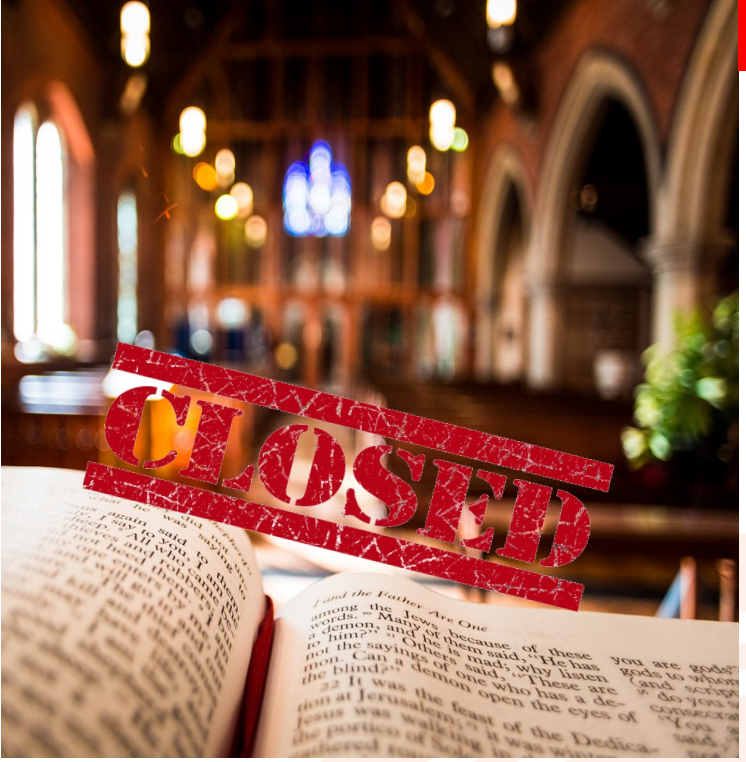

HOLD PHASE

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 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.

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.