

# 10 ESSENTIALS OF CYBERSECURITY



In today's digital world, the need to protect your organization's data and systems is crucial. The following are 10 essential measures you should take to guard against digital attacks.

## 1 Internet use and access policy

Create a written Internet Use and Access Policy and provide training on the policy to all staff and volunteers. Review the policy annually to ensure it is up to date and addresses the needs of your organization.

## 2 Employee Training

Provide cybersecurity training to your employees upon hire and periodically throughout the year. This training should include how to handle and protect sensitive information; and how to identify phishing, spear phishing, ransomware and other malicious emails. Remote staff should be made aware of best practices to keep information and data safe – e.g., routinely changing their router passwords at home, setting up a guest network for visitors, etc.

## 3 Strong passwords or passphrases

Stress the need for creating strong passwords or passphrases by using a combination of capital and lowercase letters, numbers, symbols or special characters. Never share passwords or passphrases, avoid using the same password or passphrase on multiple accounts and change them at least every three months. Remote workers should be sure to apply these same principles to their Wi-Fi passwords and passphrases when working from home.

## 4 Multi-Factor Authentication

Use Multi-Factor Authentication in addition to passwords or passphrases, along with a VPN for an added layer of protection for your internal systems and data.

**5****Keep a Clean Computer or Device**

Keep software and apps on all internet-connected systems up to date and delete unused apps to reduce the risk of infection from malware or ransomware. Regularly review app permissions to ensure they are correct.

**6****Back Up Critical Information**

Regularly back up information that is critical to the operation of your organization, or automate backups to the cloud or off-site.

**7****Network Security**

Require permission to access your Wi-Fi network and do not broadcast your network name (SSID – Service Set Identifier). Lock out accounts after multiple unsuccessful login attempts and after a pre-determined amount of time. Use firewalls and encryption to restrict access to the network and data, and use active system monitoring and penetration testing.

**8****Background Checks**

Complete criminal background checks on all individuals who have access to your systems and devices. Set criteria for what is acceptable within an individual's background to allow system access.

**9****Control Access to Your System and Devices**

Allow system and device access only to those who have been approved. Use authority levels to limit access to sensitive or critical data.

**10****Prepare for an Attack**

Prepare for an attack by reviewing and evaluating the vulnerability of all computer-related systems within your organization. Have a plan to address any vulnerabilities that are identified and review your insurance coverage for Data Breach Protection.

**Don't have these essentials covered?**

Our consultants are available by phone or email to discuss your questions and concerns.

Contact **Risk Control Central** today.

[RiskConsulting@churchmutual.com](mailto:RiskConsulting@churchmutual.com) • (800) 554-2642 EXT. 5213

PROTECTING  
THE GREATER  
GOOD™



The information contained in these materials is intended solely to provide general guidance on topics that may be of interest to you. While we have made reasonable efforts to present accurate and reliable information, Church Mutual Insurance Company, S.I. (a stock insurer)<sup>1</sup> and its affiliates disclaim all liability for any errors or omissions or for any actions you take or fail to take based on these materials. The information provided may not apply to your particular facts or circumstances; therefore, you should seek professional advice prior to relying on any information that may be found in these materials.

<sup>1</sup>Church Mutual® is a stock insurer whose policyholders are members of the parent mutual holding company formed on 1/1/2020. S.I. = a stock insurer.

CM0062 (11-2024)

NAIC # 18767; CA Company ID # 2867-0  
© 2024 Church Mutual Insurance Company, S.I.