CYBER INCIDENT REPORTING

IMPORTANT: The first few minutes and hours after learning of a cyber incident are critical to a successful recovery. The following is intended to help you and your organization know how to identify and report a suspected or actual cyber security breach.

Immediately notify your IT Resource Personnel.

During business hours, contact Jeff Schneider, Director of Claims for CMG:

402-514-2404 (Office)   402-490-0021 (Cell)

After hours contact our cyber insurance experts at NAS Insurance:

1-888-627-8995 – Identify yourself as a Catholic Mutual Member

Additionally, the following steps can help to mitigate possible issues:

Cyber Event	Immediate Mitigation Steps
Ransomware infection	• Isolate infected computer from all networks (by unplugging network cable and/or turning off Wi-Fi) • Take picture of the ransomware message on screen (if possible) • Contact your IT department • Do not immediately rebuild your system (you might destroy important forensic evidence) • Contact CMG Claims
Phishing email attack	• Do not click on link or open any attachment from suspicious email • Call IT representative and forward email to IT for evaluation • Take picture/screen shot of email request/solicitation • Change your email password (strong and unique passphrase) • Contact CMG Claims
Malware infection	• Notify IT to have them evaluate and remove malware • Scan network for any other unauthorized files and user accounts • Install anti-virus software and keep updated • Contact CMG Claims

Discovery of unauthorized files or user accounts on server or client	• Close Remote Desktop Protocol (RDP) ports • Change passwords (strong and unique passphrase) • Contact CMG Claims
Lost or stolen device	• Report lost/stolen device to IT immediately • Secure all devices and removable media (passwords and encryption)
Mistaken wire transfer	• Call bank and report details • Attempt to halt transfer • Take picture/screen shot of email request of fund transfer • Contact CMG Claims