Policy #: Remote Access

Governed by: IT Administration	
Approval Date: November 1, 2016	**Last Updated:** February 2022
Purpose: Remote Access Granted	

CEO Data Granted Remote Access

Remote access is defined as when a user requires access to the network while off-site, i.e. working from home or away from the office. To ensure that access to the network remotely is managed appropriately, it is important that we must adhere to the following:

- Non-exempt staff looking to access the CEO Network remotely must have supervisory approval for remote work.
- Only users that require remote access as part of their job role will be granted access to the network through a WatchGuard VPN license. Steps for installation will be:
    - IT grants staff member VPN license in accordance with personal access list
    - Staff Download WatchGuard VPN App to mobile device
    - IT installs WatchGuard VPN on laptop
    - Staff logs into VPN with Network name and password and verifies identity through the mobile MFA.
    - On a daily basis, login will require staff to enter a network password in the WatchGuard VPN program, and verify through the WatchGuard MFA app.
- Remote access to email will be available with the use of the Online Web Portal, which will require staff to utilize Multi Factor Authentication with every login.
- Remote access is normally available 24 hours a day 7 days a week for emails and network access. Remote login to email can be obtained by following a link from CEO's Intranet.
- Both email and network access are subject to availability, i.e. maintenance may be carried out if deemed appropriate by the IT Department and sufficient notification will be provided to users wherever technically possible.
- CEO owned property are not to be used for personal business or entertainment.
- Computers and/or mobile devices that are not owned and/or adequately controlled by CEO are not permitted for use with CEO's network and IT systems.
- Use of CEO IT property is restricted to authorized personnel only.
- While working remotely, CEO owned IT property must not be left unattended in a vehicle within plain sight of passersby.
- The loss or theft of any CEO owned IT property must be reported to CEO immediately, but only after physical safety of personnel and family members is assured.