Cybersecurity and Data Privacy

Guidelines for Working Securely While Working Remotely

Given the current COVID-19 pandemic and the various state and federal guidelines regarding stay-at-home directives, there are a record number of individuals currently working remotely. ***To reduce the threat of a security breach to your systems, secure remote access should be strictly controlled.*** *Following are additional guidelines that should be closely followed to help maintain a secure remote work environment:*

Confidential Information Awareness

- *Customer, employee and other personal and company data need to be kept secure at all times while working remotely. If confidential data must be emailed or shared,* ***USE ENCRYPTION****.*

Proper Tools

- *To the extent possible, use only business approved and issued devices. If there are any questions about proper usage, please elicit assistance from the Help Desk.*

Passwords and Multi-Factor Authentication

- *Protecting access into systems and tools is critical. Use passwords, facial recognition and/or multi-factor authentication to increase security.*
- *At no time should any person with remote access privileges provide their user name or password to anyone, including family members.*
- *Change default passwords on home equipment such as routers.*
- *Use password manager tools to help keep passwords secure, using complex passwords and avoiding the use of the same passwords across multiple accounts.*

Document Printing

- *A home environment is not the safest place for printing customer, personnel or company business documents.*
- *Printing should be restricted; when required, use a shredder to discard promptly.*

Document Sharing and Storing

- *Do not store confidential customer or personnel documents, communications and other digital information outside the company's secure environment.*
- *Do not save any confidential emails and documents directly on a personal device (they should be stored only on the company's approved storage solution using remotely accessed digital workspace/VPN or other approved personal cloud service accounts).*

Work Devices Should Not Be Shared

- *Company phones, iPads and laptops should not be shared with family members or others as there are risks associated with sharing.*
- *Strong passwords (15 characters and passphrases) should be used and changed frequently during the course of the remote-working period.*

Personal Devices Should Be Secure

- *Personal devices do not have the same perimeter controls and virus detectors that a company often has. In fact, malware may already be on these devices shared by a family.*
- *Therefore, for individuals who do not have an organization-issued device AND MUST use these personal devices, please contact your Help Desk for assistance in connecting. However, you MUST have basic tools such as antivirus, encryption, updated software and patching, password managers, multi-factor authentication, VPNs, etc. installed before gaining remote access to the organization's network.*
- *If you require assistance on how to use the company's remotely-accessed workspace, please contact your Help Desk.*

Do Not Use an Unsecure Publicly Available Wi-Fi or Home Wi-Fi Connection that Lacks Strong Password Protection

Cleansing

- *Be prepared to clear data on devices and stored in the Cloud on a regular basis, such as weekly, while working remotely.*

Be Aware of Your Online Cyber Hygiene

- *Do not click on suspicious links, especially if related to a coronavirus theme. Cyber criminals are expecting you to click without thinking.*

Designate an Incident Response Team

- *This is a prime time for cyber attacks. Companies are encouraged to designate a team of individuals who will be the front-line of responding to any type of breach. This typically includes the CEO and COO, and members from IT, security and communications. If you suspect an incident may have occurred, contact the Incident Response Team as soon as possible.*

For more information, please contact:
Karen Painter Randall
Chair, Cybersecurity and Data Privacy Group
krandall@connellfoley.com
973.840.2423

CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938