FOLEY
FOLEY & LARDNER LLP

EMPLOYEE INFORMATION SECURITY CHECKLIST

Employees are the front line of your information security defense. While technological protections are essential (for example, anti-virus software, firewalls, spam filters, etc.), none are as effective as a vigilant end user. We have created these checklists covering measures that every user should know and understand. By sharing them with individuals within your organization, you can dramatically increase not only the security of your systems and data, but the user's own personal computers and data. All too frequently, the security of one can impact the other.

KNOW YOUR DATA AND WHERE IT RESIDES

□ Know what data you have and where it is located: Ask people to show you how they create, access, and destroy data.

□ For your personal home accounts, understand where your information is stored. For example, will your data be automatically backed up to online services (e.g., Dropbox, iCloud, Microsoft OneDrive, Google Drive, SugarSync, etc.)? Do you use online document services like Microsoft Office 365, Google Docs, and others? If you use any of these services, understand how your data is protected. In many instances, your data, documents, pictures, voicemail, etc. will not be stored in encrypted form. In still other cases, the terms of use for those services may grant the provider an unqualified right to use — and even sell — your data to others. "Free" services come at a price: your privacy.

□ All confidential, proprietary, and sensitive information should be encrypted or otherwise secured.

□ Determine whether removable media is allowable. If not, disable ports and file sharing. If allowed, require information be encrypted and secured. When done with the information/device, ensure information is securely erased. Beware: If not properly done, erased or deleted information can be readily retrieved using free tools from the Internet.

□ Never transfer sensitive company information to a mobile storage device (e.g., a CD, USB drive, etc.) unless expressly permitted by our security policies and procedures.

□ Consider purchasing credit monitoring protection for your personal information. Among other things, these services will continuously monitor the Internet — particularly known hacking sites — for evidence of your personal information (e.g., social security number, credit card numbers, phone number, etc.).

FOR MORE INFORMATION

Michael Overly
Partner
Los Angeles, California
213.972.4533
moverly@foley.com

Eileen R. Ridley
Partner
San Francisco, California
415.438.6469
eridley@foley.com

Chanley Howell
Partner
Jacksonville, Florida
904.359.8745
chowell@foley.com

MONITOR

□ Monitor activity within the network and your systems.

□ Review abnormal behavior (e.g., a user that normally always works days, logging in during the middle of the night).

□ Encourage users to report concerns and to ask questions.

VENDORS, SERVICE PROVIDERS, CONSULTANTS, AND OTHER THIRD PARTIES

□ Never allow a third party to use a workstation or otherwise access or use your systems and data without supervision and appropriate contractual protections.

□ Conduct due diligence of all service providers and ensure they are compliant with applicable law and our corporate security requirements.

□ For your personal home devices (e.g., laptops, tablets, smartphones, etc.), consider removing sensitive unencrypted data before having a third party service the device. There have been many instances where individuals have brought their laptops and other devices to a local computer repair shop for service only to find out the operator of the store secretly stole their data. Use care when granting a computer or warranty vendor access to your computer for tech support. In many instances, once access is granted, they will have access to the entire content of the hard drive, and in some cases the network, if the computer is connected to the network.

□ If you sell or otherwise dispose of a personal device, make sure your data is securely removed/deleted from the device. Simply deleting files is not sufficient. They can be easily recovered. There are readily available programs on the Internet to securely delete data. In addition, doing a full reset to “factory condition” on a smartphone will erase all data.

ONLY AUTHORIZED SOFTWARE

□ Do not download or install unauthorized or unapproved software or applications from the Internet.

□ In particular, never install encryption software, remote access, backup, or other similar software without the express approval of our information security personnel.

□ Always be certain of the source of downloaded software (i.e., you are actually getting the software from its true creator). It is common for hackers to create fake websites and even “hijack” visitors from official websites, where applications can be downloaded. In some instances, the top search results for software on Google and other search engines point to disguised hacker websites, where your personal information may be stolen and viruses propagated.

□ For your personal computers, make sure you have anti-virus and firewall software installed. There are many inexpensive, complete security packages available for home systems. Also, always promptly install security and other updates to your personal computer and mobile device operating systems.

WEBSITES, SOCIAL MEDIA, AND PUBLIC EMAIL

□ Always proceed with the understanding that no public email or messaging service (e.g., services provided by online services such as Google, Yahoo!, Microsoft, Skype, and others) is secure, and that all communications will be stored and, potentially, viewed by others.

□ Avoid sending highly sensitive information through unsecured email, texts, or other communications (e.g., Gmail, Yahoo! mail, text apps on smartphones, etc.).

□ Do not forward internal email, documents, or other information to a personal email address or download to personal devices for access outside of our systems. We cannot protect the information once it has been removed or shared outside of our systems.

□ When submitting personal or other sensitive information via a website, make sure you see the site's address begin with "https," as opposed to "http." Think "s" stands for secure. "Https" uses encryption to send information across the Internet, thus, reducing the risk that the information will be improperly accessed.

□ Think before you submit. Once submitted to a website or transmitted through an online communication service, the information is public. You never know where the information will show up. There is no such thing as deleting information from the Internet. The Internet is forever.

□ Exercise caution using services and devices that record your communications (e.g., Google Voice, Siri, Microsoft Cortana, Skype, VoIP applications, mobile app-based texting, etc.).

□ Before posting pictures and videos online, remember they may contain GPS data showing where the picture was taken.

□ Be mindful of backup applications running on personal devices (e.g., Dropbox, iCloud, Carbonite, etc.), making copies of sensitive company information, and storing them online.

□ Do not get hooked on someone's fishing line. Do not reply to or click on links in emails, pop-ups, or websites that ask for personal information, financial information, or health information. Never click on links or open files in an email from someone you do not know or were not expecting.

□ Think before you open. If you do not know the sender, are unsure of why the attachment was sent, or if it looks suspicious, do not open the attachment. Better to verify with the sender than infect your computer, or worse, the network.

□ PDF files are a very popular way of distributing viruses. Before opening a PDF, be sure you know where it came from.

□ When installing apps on your smartphone, be cautious of requests to access your calendar, contacts, texts, GPS, and other data. In many, if not most, instances, there is no reason for these apps to have access to your data and, in almost all instances, whatever you choose to share will likely be analyzed and sold to others.