## Workstation Security

Protecting your workstation area - specifically your desktop computer and other supporting devices - is an important duty all employees should take very seriously. While many of the workstation security best practices mentioned below are also discussed in other areas of the security awareness training program, you'll find additional requirements, tips, and suggestions considered important. Employees spend long hours at their workstations, so it's critical to implement the following best practices:

- **It's your workstation.** That means only you should be using it, and primarily for business purposes only. Sure, it's fine to conduct personal activities also, such as checking your email, logging into online banking, even accessing a few of the accepted social media platforms, such as Facebook and LinkedIn. Allowing other employees to use your workstation is strictly prohibited, so be aware of this. Imagine another employee using your workstation, accessing the Internet and possibly downloading unsuspected malware, sending an unprofessional email, or any other action? It happens all the time and you don't want to be blamed for something you didn't do, so don't share your workstation rights.

- **Use strong passwords.** While most passwords will be enforced by group policy settings from I.T. personnel, it' still important to make them unique, never using information pertaining to your favorites sports team, home address, middle name, etc. With password complexity requirements in place often requiring the use of symbols and numbers and other mandates, it's also a good idea to adopt the same policies to other systems and websites that you personally have administrative password access right to, such as online banking, social media accounts, or any business accounts that are not group policy enforced by I.T. personnel.

- **Security updates.** Make sure your workstation computer has all the required security updates for the operating system and all other applications running. This also means having anti-virus running at all times and conducting periodic scans. Additionally, the use of anti-spyware may also be required as it provides additional layers of protection, especially during Internet usage. While most of the security updates are "pushed" out and managed by I.T. personnel, at times you'll still need to accept these updates.

- **Don't alter security settings.** Your workstation has been configured for maximum security along with performance, so do not attempt to disable or modify configuration settings to the operating system or any other applications. Doing so may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts to reside on the workstation.

- **Don't install any unapproved software.** Your workstation has also been configured for providing you the necessary tools in performing daily roles and responsibilities, which means no additional software is needed. Do not download or install into any of the drives or ports additional software that has not been approved as it may contain malicious files, could consume additional resources, or is simply not professionally suitable for the work environment.

- **Removable storage devices.** They're easy-to-use, inexpensive, and a great way for transferring information, yet they're also incredibly dangerous when the wrong information is on them and in the wrong hands. With that said, USB ports, such as thumb drives, external hard drives, and other removal storage and memory devices are never to contain highly sensitive and confidential information, such as Personally Identifiable Information (PII), or any other data deemed privileged. Such information should be transferred over the network using approved protocols and residing on company servers only.

- **Use caution with email.** Be careful when opening emails from unknown parties, especially attachments. If it looks suspicious, do not open the email under any circumstances. Additionally, avoid clicking on links or banner advertisements sent to you as these often containing spyware, malware, etc.

- **Be mindful of Instant Messaging.** Instant messaging is considered fun, informal, and an easy and affordable way to communicate – all of which are true. Just be very careful as to the types of information you're sending and receiving via instant messaging, which ultimately means not transmitting any type of highly sensitive, confidential, or privilege information. This includes what's commonly known as Personally Identifiable Information (PII) – unique identifiers for any individual, such as social security numbers, dates of birth, medical accounts, etc. If you're not sure as to the sensitivity of the information, don't send it over IM.

- **Handle privileged information with care.** From emails containing sensitive information to hard copy documents for contracts, trade secrets, or any other type of confidential data, treat it with the utmost care and professionalism, making every effort to protect its confidentiality and integrity. Don't divulge such information to unintended parties and never leave items (both hard copy and electronic media) unattended in public at any time (i.e., coffee shops, training seminars, conferences, etc.).

- **Report security issues immediately.** Remember, if you see something, say something – and immediately. You have a responsibility for helping protect the organization, which means being aware of your surroundings and reporting suspicious activity to authorized personnel – immediately. From seeing a door ajar that shouldn't be to finding sensitive documents lying in a commons area, you need take action.

- **Shut down and protect your workstation.** When leaving your workstation area at the end of each day, make sure to completely shut down and turn off all computers and related devices. Additionally, pickup and store any documents, electronic media, or any business and/or professional items that should not be left unattended. Use your judgment by asking yourself the following simple question – "what risk or security danger is there for leaving something not securely locked up and put away?"

## Laptop Security

Securing your laptop at all times is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, your laptop is a constant source of target, so beware. Take the following precautions for securing what's arguably one of your most important possessions:

- **Use Encryption.** The use of full-disk encryption ensures that safety and security of data (i.e., user files, swap files, system files, hidden files, etc.) residing on your laptop, especially if it's stolen, lost, or misplaced.

- **Use Anti-virus.** It's one of the most fundamentally important – and often not used – security software, so make sure your laptop has anti-virus running at all times, along with its scanning at regular intervals for viruses, and that the software is current.

- **Turn on your firewall.** Blocking suspicious traffic is essential for laptop security, so turn on and "enable" your default personal firewall or an approved personal firewall software appliance, for which there are many available.

- **Use strong passwords.** When turning on your laptop, your initial password should be extremely strong, with a combination of letters, numbers, and symbols used. Once your initial password is compromised, the contents of your entire laptop (especially if you're not using full-disk encryption) can be compromised. Don't use terms and phrases for which somebody might find an association with you, such as favorite football team, home address, middle name, etc.

- **It's your laptop.** Therefore, don't let other individuals use it, especially if it's somebody you don't know. When situations arise that require it to be used by someone other than you, create a guest account for their use.

- **Secure it physically.** A good investment is a security cable with a lock for securing your laptop at a workstation or any other location that requires such. They're relatively inexpensive and a great deterrent to any thief.

- **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe. That means not using the coffee house phrase "can you watch my laptop for a minute as I go to the restroom", or any other similar thought process. Being vigilant and watchful at all times is a must for the safety and security of your laptop, so remember – do not leave it unattended – plain and simple. If you have to leave in your hotel room or some other location, then remove it from sight and place under a pillow, in a closet, or some other location. The best safety measure is to carry it with you at all times.

- **Place your contact information somewhere visible.** Because most people are honest and trustworthy, should your laptop be stolen, misplaced or lost – and then subsequently found by a

good Samaritan – you'll clearly want your name, phone number, address, and/or email visible on it. Put a sticker on the cover or back of your laptop with all your relevant contact information.

- **And if your laptop is stolen.** Laptops unfortunately do get stolen, so think and act quickly, which means reporting the theft to local authorities along with informing management (and the I.T. department) immediately.

## Software Licensing and Usage

It's also important to understand the company's general policy on software usage, which includes numerous responsibilities that all employees need to be aware of. Software is used by all of us, each and every day, as it's vital to performing daily tasks for one's job function. With that said, please be mindful of the following issues:

- **Use only approved software.** Only software approved and purchased from the company may be installed and used on any company-wide system components. This includes your workstation and any other device provided to you from the company. Unapproved software that has not been fully vetted by authorized I.T. personnel and can often contain dangerous or malicious code that's extremely harmful to computers. Simply stated, only load and use legally approved software on computers.

- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means you are not allowed to copy or duplicate any company approved and purchased software – no exceptions. U.S copyright laws – and other regulations throughout the world – often place strict guidelines on software usage, so please keep this in mind.

- **Use caution on your own devices.** When using your own personal workstation, laptop, or other device, please consider and be mindful of the software you install, especially when such computing systems are used for potentially accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, we still ask that you use extreme caution when loading any type of application onto your devices.

- **Accept updates.** For software to function efficiently and safely, security and patch updates have to be applied on a regular basis, so make sure to accept such updates when pushed out and also take time to update any software on your personal computers that do not rely on updates pushed out by I.T. personal.

- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements, and also comprehensively scanning the software for ensuring no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seem harmless, only to contain viruses that can wreak havoc on computers. Think before you start downloading any software online.

- **Software audits.** As an employee of the company, we have the right to conduct random software compliance audits on workstations, including laptops issued to you, or your own personal laptops. The audits are for ensuring compliance with software licensing rules, while also ensuring your computers are free of any potentially dangerous applications. If you're not sure what constitutes approved software, then simply ask somebody.

- **Penalties and fines.** Did you know that we as a company and you as an employee can actually be levied fines for improper software use? Yes, it's that serious and it's why we're taking the time to discuss this important issue with you. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages up to $150,000 (Section 504(c)(1) Title 17) per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to ten (Section 2319 (b) (2) Title 18) years.

## Encryption

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability (CIA) of [company name] system components and any sensitive data associated with them. Additionally, any passwords used for accessing and/or authentication to the specified system component are to be encrypted at all times, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such as Secure Sockets Layer (SSL) | Transport Layer Security (TLS), Secure Shell (SSH), and many other secure data encryption protocols are to be utilized when accessing the specified system component. Additional encryption measures for [company name] are to also include the following best practices for all applicable devices that have the ability to store sensitive and confidential information:

- **Servers -** Depending on the type of server and the underlying applications, a large range of encryption measures can be adopted. The first measure is identifying the type of information residing on such servers and the necessary encryption protocols to apply. Additionally, servers are to be provisioned and hardened accordingly, with anti-virus also installed.

- **Desktop Computers -** Any desktop computer storing sensitive and confidential information are to utilize encryption for the actual hard drives. Additionally, access rights are to be limited to authorized personnel at all times. Non - [company owned] desktops, such as those physically located at an employee's home, are to never contain sensitive and confidential information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the [company name] network for accessing all relevant information. Additionally, desktop computers are to be provisioned and hardened accordingly, with anti-virus also installed.

- **Laptops, Mobile Computing Devices, Smart Devices -** Such devices are to have approved encryption installed and enabled prior to their use, which requires [company name] authorized I.T. personnel to configure appropriate encryption programs. Specifically, full disk encryption, or other approved methods, such as file level encryption are to be used, and these devices are not to be used

for long-term storage of sensitive and confidential information. The phrase "long term" is discretionary in nature, but consists of any data residing on laptops, mobile computing devices, and smart devices longer than thirty (30) calendar days. Non - [company owned] laptops, mobile computing devices, and smart devices, are to never contain sensitive and confidential information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the [company name] network for accessing all relevant information. Additionally, laptops, mobile computing devices, and smart devices are to be provisioned and hardened accordingly, with anti-virus also installed.

**Removable Storage Devices -** USB enabled devices, such as memory sticks, external hard drives, network attached storage devices are strictly prohibited. Though there may be circumstances that require storing of sensitive and confidential information onto these utilities, it must be approved in writing, and such data is never to reside on these devices for long-term storage measures.

- **Unknown Devices** - The phrase "unknown devices" is given to such items as kiosks, hourly computing stations for rent, friends and family members computers, or any other types of device for which [company name] has little to no knowledge regarding its safety and security. These devices are never to be used for storing, processing or transmitting sensitive and confidential information due to the lack of knowledge of their respective encryption practices, which many times are none at all.