INFORMATION SECURITY POLICY

Contents

1. Workstation Security

Protecting your workstation area - specifically your desktop computer and other supporting devices - is an important duty all transcribers and 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 programme,

additional requirements, tips, and suggestions will be circulated from time-to-time, all of which are considered important. Transcribers spend long hours at their workstations, so it's critical to implement the following best practices:

It's your workstation

That means ideally only you should be using it, and primarily for business purposes only. Be careful who has access to your laptop - imagine someone using your workstation, accessing the Internet and possibly downloading unsuspected malware, sending an unprofessional email, or any other action? It happens all the time.

Use strong passwords

While most passwords will be enforced by group policy settings from IT, it's still important to make them unique, never using information pertaining to your favourite 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 IT.

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.

Security settings

Ensure your workstation has been configured for maximum security along with performance.

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 contain spyware, malware, etc.

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 removable storage and memory devices are never to contain highly sensitive and confidential information, such as Personally Identifiable Information (PII), transcripts, recordings, or any other data deemed privileged. Such information should be transferred using Sharefile/Global Lounge and other approved client servers only, unless you are using previously agreed encrypted USB sticks.

Be mindful of Instant Messaging

Instant messaging, including Slack, 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/Slack, 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/hear something, say something – and immediately. You have a responsibility for helping protect the organisation, which means being aware of your surroundings.

Shut down and protect your workstation

When leaving your workstation area, make sure to completely shut down and turn off all computers and related devices. Additionally, pick up 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?”

2. 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. Take the following precautions for securing what's arguably one of your most important possessions. 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 softwares, 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.

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) is at risk. Don't use terms and phrases that somebody might associate with you, such as favourite 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 where possible.

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.

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 want your name and phone number visible.

3. Software Licensing and Usage

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

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 dataset. This means you are not allowed to copy or duplicate any company approved and purchased software – no exceptions.

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. We 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 IT.

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 to ensure no dangerous or malicious code exists. Think before you start downloading any software online.

4. Encryption

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability (CIA) of McGowan Transcriptions' 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. Additional encryption measures for McGowan Transcriptions are to also include the following best practices for all applicable devices that have the ability to store sensitive and confidential information:

Desktop Computers

Any desktop computer storing sensitive and confidential information are to utilise encryption for the actual hard drives. Additionally, desktop computers are to be provisioned and 'hardened' accordingly, with anti-virus also installed. You will be requested to inform McGowan Transcriptions of all security packages implemented and upgrades on a yearly basis via the Compliance Manual.

Laptops, Mobile Computing Devices, Smart Devices

Such devices that are used for McGowan Transcriptions are to have approved encryption installed and enabled prior to their use. 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-McGowan Transcriptions or client-owned laptops, mobile computing devices, and smart devices, are to never contain sensitive and confidential information under any circumstances that relate to McGowan Transcriptions or its clients. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the Sharefile network for accessing all relevant information. Additionally, laptops, mobile computing devices, and smart devices used for transcripts are to be provisioned and 'hardened' accordingly, with anti-virus also installed.

Emailing

Transcribers must download all files using Sharefile, Global Lounge, Citrix system or client SSTP site where applicable. Some clients allow us to email files without encryption, you will be made aware for each project where this applies.

Removable Storage Devices

USB enabled devices, such as memory sticks, external hard drives, network attached storage devices are strictly prohibited for use with McGowan Transcriptions information unless they are encrypted sticks. 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 of which McGowan Transcriptions 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, of which many times there is none at all.

Confidentiality Agreements

All Transcribers are to sign the McGowan Transcriptions Transcriber's Confidential Disclosure Agreement, which must be reviewed and signed every year along with our Compliance Manual.

Declaration

You are responsible for adhering to our Information Security Policy, please sign below to acknowledge that you have read and understood your responsibilities regarding the McGowan Transcriptions Information Security Policy.

Signature: _____

Name (in block capitals): _____

Date: _____