Cyber Security Policy

WHAT IS THE PURPOSE OF THIS DOCUMENT?

JOS Structures Limited (from here on referred to as The Company) has noted the ever-growing importance of proper Cyber Security measures in the workplace. This policy outlines the measures that The Company and its employees shall commit to, in order to protect the interests of The Company, its employees, and any third-parties it interacts with.

WHAT IS CYBER SECURITY?

Cyber Security is the practice of protecting IT systems and equipment from attacks and exploits by malicious actors. IT systems and equipment can refer to hardware (computers, hard drives, mobile phones, etc.), software, networks, etc.

These kinds of attacks are becoming increasingly common and it is the responsibility of users of IT equipment at all levels of The Company to ensure they are adhering to the measures outlined below.

WORK STATION SECURITY

Protecting your workstation area is an important duty all users should take very seriously.

- It is your workstation. That means that only you should be using it, and primarily for business purposes only. Allowing other JOS Structures Ltd employees to use your workstation is strictly prohibited. Do not let anyone have unsupervised access to your workstation. Imagine another employee using your workstation, accessing the Internet and possibly downloading unsuspected malware, sending unprofessional e-mails, or any other unwanted action. It can and has happened with companies, and you don't want to be blamed for something you didn't do, so do not share your workstation rights.

- Use strong passwords. Passwords are used as a means to secure your workstation, and the software that runs on it, from any unauthorised access. It is important to make your passwords unique, do not use any personal information as your password. Use letters, numbers and symbols within your password--that way it will make it complex and secure. It will very likely be that your password for your IT

workstation, software logins and so on, will have been already generated and allocated to you. Do not reuse the same password for multiple different accounts.

- Security Updates. Make sure your workstation 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 use.

- Do not alter security settings. Your workstation has been configured for maximum security along with performance, so it is strongly advised that you do not attempt to disable or modify the configuration settings to the operating system or any other applications. By doing so you may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts reside on your workstation.

- Do not 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, and 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 can also pose a serious threat when the wrong information is stored on them and in the wrong hands. Having said that, USB ports, thumb drives, external drives and other removable storage and memory devices should never hold and 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 E-mail. Be careful when opening e-mails from unknown parties, especially attachments. If an e-mail looks suspicious, then do not open it under any circumstances. Additionally, avoid clicking on links or banner advertisements sent to you as these often contain spyware, malware, etc.

- Be mindful of Instant Messaging. The use of Instant Messaging software on Company IT systems is expressly forbidden.

- Report security issues immediately. Remember, if you see something, say something immediately. You have a responsibility for helping protect the Company, which means being alert to any unusual behaviour on your system or any other possible signs of malicious attacks, and reporting these suspicions to authorised personnel immediately.

- Shut down and protect your workstation. When leaving your workstation area at the end of each day, make sure that you completely shut down and turn off all computers and related devices. Additionally, pick up and store any CDs, thumb drives, or hard drives, etc. that should not be left unattended.

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 target for malicious activity, so beware. Take the following precautions for securing what's arguably one of your most important possessions:

- Use encryption. The full-disk encryption ensures the safety and security of your data (i.e., user files, swap files, system files, hidden files and so on.) residing on your laptop, especially if it is stolen or misplaced.

- Use anti-virus. It's one of the most fundamentally important - and often not used - pieces of security software, so make sure your laptop has anti-virus software running always, along with it scanning for viruses and other malware at regular intervals. Also ensure that the anti-virus software is current and is updated regularly.

- 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.

- 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 are not using full-disk encryption) can be compromised. Do not use terms and phrases for which somebody might find an association with you as your password, such as favourite football team, home address, middle name and so on.

- It's your laptop. Therefore, don't let other individuals use it, especially if it is 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.

- Keep a watchful eye. Don't ever leave your laptop unattended in any public venue or location not considered safe. Being vigilant and watchful always is a must for the safety and security of your laptop, so remember - do not leave it unattended - plain and simple. The best safety measure of all is to carry it with you always.

- 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 someone - you should clearly display your name, company telephone number, company address and e-mail on the laptop. Such information can be put on a sticker on the cover lid or the bottom of the laptop.

- And if your laptop is stolen. Laptops can and do get stolen, so think and act quickly, which means reporting the theft to the Police along with informing The Company's management team 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 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 for The Company from a reputable software house and retailer should be installed and used on Company IT equipment. This includes your workstation and any other device provided to you by the Company. Unapproved and unlicensed software can contain dangerous or malicious code that can pose a serious threat to the Company's IT infrastructure. Simply stated, only load and use legally approved software on Company 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 that you are not allowed to copy or duplicate any Company approved and purchased software - no exceptions. Copyright laws - and other regulations around 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 accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, you must still exercise 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 you must ensure that you accept such updates when they are generated and distributed and also take time to update any software on your personal computers.

- 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 that no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seems harmless, only to contain viruses, and other malicious code that can wreak havoc on IT systems. Think before you start downloading any software online.

SIGNED *J O' Sullivan*

DATE 23rd August 2024