DEFINITIONS:

Vulnerability: (in the context of Cybersecurity) a weakness, usually in design, implementation or operation of software (including operating systems), that could be compromised and result in damage or harm.

Data: Information stored in a digital or electronic format.

Risk: A situation involving exposure to significant impact or loss. In formal frameworks, risk can be quantified using probability (often expressed as a percentage) and impact (often expressed as a financial amount). Other parameters for risk can include proximity (how soon a potential risk may be encountered, and information about which assets, services, products and processes could be affected).

Threat: Any source of potential harm to the digital landscape. Whether intentional or accidental. A glass of water, a malicious line of code.

Digital landscape: The collection of digital devices and electronic information that is visible or accessible from a particular location.

Defense in Depth: The use of multiple layers of security techniques to help reduce the chance of a successful attack. The idea is that if one security technique fails or is bypasses, there are others that should address the attack. The latest (and correct) thinking on defense in depth is that security techniques must also consider people and operational factors (for example processes) and not just technology

Control Policy: (in the context of security and compliance) a method of regulating something, often a process, technology or behavior, to achieve a desired outcome, usually resulting in the reduction of **risk**. Depending on how it is designed and used, any single control maybe referred to as a preventative, detective, or corrective.

Protocol: (In the context of electronic communications) is a set of established rules used to send information between different electronic locations. Protocols provide a standard that can be used to send or receive information in an expected and understandable format, including information about the source, destination, and route.

VPN: (Virtual Private Network) A method of providing a secure connection between two points over a public (or unsecure) infrastructure; for example, to set up a secure link between a remote company laptop in a hotel and the main company network.

Assessment: The evaluation of a target (for example an application, service, or supplier) against specific goals, objectives or other criteria through the collection of information about it. Usually, this is achieved through an established and repeatable process that involves discussing or answering questions about the target's capabilities and approaches. The purpose is to understand how closely the target meets the intended criteria and to identify any gaps or deficiencies. An assessment is different than an

audit because it does not necessarily check for evidence (or proof) that the responses are genuine and does not need to be carried out by an objective third party. It can be considered that a security assessment is usually akin to a consultative audit that does not seek to catch out or disprove the evidence provided by the target being examined.

Convention: The usual way or accepted way of behaving, especially in learned behaviors, often following an old way of thinking or a custom way learned in the past. A formal agreement between a vendor and a user.

Default Account: Generic user and passwords with standard permissions, often with administrative access that is provided as standard for some applications and hardware for use during initial setup.

Encryption: The act of encoding messages so that if they are intercepted by an unauthorized party, they cannot be read unless the encoding mechanism can be deciphered.

Attack: The occurrence of an unauthorized intrusion.

Adware: any computer program (software) designed to render adverts to an end user. This type of software can be considered a form of malware if: (1) the advertising was not consented by the user, (2) if it is made difficult to uninstall or remove, or (3) if it provides other covert malware functions.

Malware: Shortened version of malicious software. A term used to describe disruptive, subversive or hostile programs that can be inserted onto a digital device. People can intentionally or unintentionally make these types of programs harmful.

Scareware: Malicious software that is designed to persuade people to buy an antidote for a computer infection. It usually masquerades as a commercial malware removal tool or anti-virus package. But in reality, it is provided by the attacker and may steal data, track your usage, and allow unauthorized access into your computer.

Ransomware: A form of malicious software (malware) that prevents or restricts usage of one or more digital devices or applications or renders a collection of electronic data unreadable until a sum of money is paid.

Trojan: An application (software program) that appears to be harmless, but that actually hides and facilitates the operation of other, unseen malicious and unauthorized software programs and activities.

Anti-Malware / Anti-Virus: Is a computer program designed to look for specific files and behaviors (signatures) that indicate the presence or the attempted installation of malicious software. If or when detect, the program seeks to isolate the attack (quarantine or block the malware), remove it, if it can, and also alert appropriate people to the attempt or to the presence of the malware. Newer versions of anti-malware use machine learning and make use of additional techniques including behavior monitoring.

BYOD: (Bring Your Own Device) indicating that employees and other authorized people are allowed to bring some of their own digital devices into the workplace – or take home – to use for some work purposes.

Virtual Machine / Desktop: A computer with an operating system that can run applications but that does not physically exist. Instead of running on an exclusive piece of physical hardware, the computer is merely a set of software and configuration files. A virtual desktop is a virtual machine that emulates the functions of a personal computer. Virtual machines are often used for security purposes, as they are quick to clean, easy to set up and useful for isolation threats.

Cybersecurity: The protection of digital devices and their communication channels to keep them stable, dependable and reasonably safe from danger or threat. Usually the required protection level must be sufficient to prevent or address unauthorized access or intervention before it can lead to substantial personal, professional, organizational, financial and /or political harm.

Exploit: to take advantage of a security vulnerability. Well-known exploits are often given names. Falling victim to a known exploit with a name can be a sign of low security, such as poor patch management. [or no antivirus protection]

Patch management: A controlled process used to deploy critical, interim updates to software on digital devices. The release of a software 'patch' is usually in response to a critical flaw or gap that has been identified. Any failure to apply new interim software updates promptly can leave open security vulnerabilities in place. As a consequence, promptly applying these updates (patch management) is considered a critical component of maintaining effective cybersecurity.

IoT: (Internet of Things) the incorporation of electronics into everyday items sufficient to allow them to network (communicate) with other network-capable devices. For example, to include electronics in a home thermostat so that it can be operated and can share information over a network connection to a smartphone or other network-capable devices.

Risk assessment: A systematic process for the proactive detection of potential hazards or gaps in an existing or planned activity, asset, service, application, system or product.

Multi-factor authentication: Using more than one form of proof to confirm the identity of a person or device attempting to request access. For example, two-factor authentication would require that when access is being requested, proof would be required from at least two different categories or devices.

Social Engineering: The act of constructing relationships, friendships, or other human interactions with a preconceived fabricated connection for the purpose of enticing the recipient to perform an action or reveal information. The individual(s) doing the social engineering use the victim's action or information for the hidden purpose of achieving a nefarious objective, such as acquiring intelligence about the security, location or vulnerability of assets, or even gaining the person's trust to open an internet link or document that will result in a malware foothold being created.

Phishing / spear phishing: Using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example, a password or credit card number) from the recipient or to install malware on the recipients device. The methods used in phishing have evolved so that the message can simply contain a link to an internet location where malware is situated or can include an attachment (such as a PDF or

Word document) that installs malware when opened. The malware can then be used to run any number of unauthorized functions, including stealing information from the device, replication additional malware to other accessible locations, sharing the user screen and logging keyword entries made by the user. Less complex, but slightly more dangerous, forms of phishing can encourage the recipient to visit a fake but convincing version of a website and to disclose passwords to other details.

Spoofing: concealing the true source of electronic information by impersonation or other means. Often used to bypass internet security filters by pretending the source is from a trusted location.