Appendix 'A'

Glossary

Anti-virus - Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, Trojans.

Back-Ups - the copying of physical or virtual files or databases to a secondary site for preservation in case of equipment failure or other catastrophe.

Cyber-Attack - an attempt by hackers to damage or destroy a computer network or system.

Cyber-Breach - a data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorised individual.

Encryption - the scrambling of sensitive information so that it becomes unreadable to everyone except the intended recipient.

Firewall - a network security system designed to prevent unauthorised access to or from a private network.

Hacker - now commonly associated with someone who uses computers to gain unauthorised access to data. Hackers can also be positive ethical process whereby someone hacks for a company or organisation to enhance defensive measures.

Malware - software which is specifically designed to disrupt or damage a computer system.

Phishing - the fraudulent practice of sending e-mails to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy source.

Ransomware - malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key.

Risk Assessment - the process of determining the likelihood that a specified negative event will occur.

(END)