Cyber Essentials Information Assurance 2025

Purpose and Scope

• To protect the Company’s data from loss, damage, or unauthorised access
• To prevent the Company’s computing resources being used for activities which are illegal, or which violate any other policies, procedures, guidelines, or standards of the Company
• To prevent damage to, or degradation of, the Company’s computing resources
• To inform employees about acceptable and unacceptable use of the Company’s computer resources.
This policy forms the basis of any computer resource usage by employees and must be read and understood before an employee can access any of the Company’s computer resources. Failure to comply with this policy could lead to disciplinary action up to and including dismissal.

Definitions

The Company’s computer resources are defined as all software, databases, workstations, PC’s, laptops, mobile phones, servers, printers, cameras, scanners, firewalls, routers, switches, network equipment, other network devices, tablets, telephones and telephone equipment and links owned, leased, or rented by the Company including online and internet services. For purposes of this policy, the term "mobile phone" is defined as any electronic device with the ability to receive and/or transmit voice, text, or data messages without a cable connection, including ‘Smart’ watches.
Users are defined as any employee or other person who uses the Company’s computing resources.
The term Internet includes www, FTP, Newsgroups, e-mail, cloud-based services, and other online services.

Security Awareness

Security belongs to everyone, and all Users should realise this and be vigilant for any breaches of security, although information security is the overall responsibility of the Company Directors. The Company's computing resources holds information, which may be highly confidential, all Users must take precautions to ensure that this information does not get into the wrong hands. It is important that any incidents that might lead to a loss of confidentiality or availability are reported to the Operations Director. Faults should also be reported in the same way.

Means of Identification

Each User likely to use the Company’s Sale Order Processing (SOP) software is allocated an identity by means of a login and password and permission level. This permission will depend on their role and responsibilities and the trust placed in them. The login will be fixed, and other people may know this, but the password proves the identity; and is to be kept a secret. Each user is responsible for all transactions made under the authorisation of their ID, and for all network activity originating from their machine.

Breaches

All employees have an obligation to report any actual or suspected system, security, or data protection breaches. This will allow Lamberts to investigate and take any necessary action. Unauthorised access by a member of staff is prohibited, and failure to abide by this could lead to disciplinary action up to and including dismissal.