

Information Security Policy

Policy Statement:

This information security policy shall apply to information, systems, networks, applications, locations and employees of the Company.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by the Company. This shall be achieved by:

- Ensuring that all the Company's employees are aware of and shall comply with relevant legislation, including the General Data Protection Regulations (GDPR), Data Protection Act (2018) and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Describing the principles of information security management and describing how they shall be implemented within the Company.
- Assisting employees to identify and implement information security as an integral part of their day to day role within the practice.
- Safeguarding information relating to clients and employees under the control of the organisation.
- The company commits to ensure that there will be culture of continual improvement on all aspects of our security system across the whole organisation.

Objectives:

Key objectives of this Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to employees of the Company and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the client, when it is needed.

Responsibilities:

- Responsibility for information security shall rest with the Managing Director. However, on a day-to-day basis the General Manager shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The General Manager shall be responsible for ensuring that both permanent and temporary employees including any contractors are aware of:-
 - The information security policies applicable to their work areas
 - Their personal responsibilities for information security
 - Who to ask or approach for further advice on information security matters.
- All employees shall abide by security procedures of the Company. This shall include the maintenance of Company records whilst ensuring that their confidentiality and integrity are not breached. Failure to do so may result in disciplinary action.

Information Security Policy

- This Information Security Policy document shall be owned, maintained, reviewed and updated by the General Manager. This review shall take place not less than annually. The results of which shall be made known to the Managing Director.
- Employees of the Company shall be responsible for both the security of their immediate working environments and for security of information systems they use [e.g. workstations, laptops, hand held computer devices, portable memory devices etc.].
- Contracts with third party organisations that allow access to the information systems of the Company shall be in place before access is allowed. These contracts shall ensure that the employees or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the Company.
- Any breach of Data Security shall be communicated to the client within 24 hours of the breach to allow the client to inform the ICO within the 72 hour timeline. Once client has been informed of the data breach the company has a further 48 hours to complete the investigation and report back to both the ICO and the client.

The Company shall undertake to ensure:


- **Contracts of Employment** – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.
- **Access Controls** - to areas containing information systems are restricted and controlled to ensure that only those authorised can access information of the Organisation. All activity is logged on the access control system and is retained indefinitely to ensure a complete audit trail.
- **Network Security** – access to the company’s computer network will be restricted and controlled to ensure only those authorised can use it. Security policies shall be in force to restrict access to specific areas of the network drives to ensure individuals only have access to the information necessary to carry out their role. All network users will have a password known only to themselves and will be required to change it every 90 days.
- **Data Backups** – All data stored within the network drives is backed up on a daily basis to a server located in separate location to ensure no loss of sensitive or business critical data in the event of fire, theft or any form of damage to the main premises.
- **Equipment Security** – Is effective in order to minimise losses, or damage to the Company. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets, clear desk policy and the limitation of risks in the surrounding work area etc).
- **Information Risk Assessment** – a regular assessment of the working environment, shall be conducted to identify potential risks to the security of the Company’s information. Where risks are identified, these should be noted and where possible mitigating action taken.
- **Security Incidents and weaknesses** - are to be recorded and reported to the Managing Director so that they can be investigated to establish their cause, impact and the effect on the Company and its clients. (NB. remedial changes arising may need to be included within future employees working procedures, updates to policies and contracts of employment).

Information Security Policy

- **Anti-Virus / Hardware Firewalls** – all workstations, laptops and mobile computing devices are protected at all times through the use of commercial strength anti-virus/anti-malware software. All internet connections to the premises shall be managed with the use of a hardware firewall. Firewall penetration testing is carried out on a 30 day basis as part of the companies PCI compliance policy and any issues discovered are immediately addressed and reported to the Managing Director. All anti-virus software and the hardware firewall shall be regularly updated via software patched supplied by their respective manufacturers.
- **Software Installations** - no new software shall be downloaded or installed on computer systems of the Company without the explicit permission of the General Manager. Breach of this requirement may be subject to disciplinary action. Updates and patches released by the software suppliers shall be applied as so as they are made available.
- **Secure Communications** – should be in place to ensure that all correspondence, faxes, email, telephone messages and movement of client information are conducted in a secure and confidential manner. All telephone and email communications are logged on their respective management systems.
- **Reporting Data Incidents** - All data incidents whether large or small need to be investigated to ensure that any lessons that need to be learnt are disseminated to all team members. The General Manager is to be included in all Data Incidents to ensure that actions that are needed are carried out in the correct timescale. Reporting of all incidents/issues is to be done via the **SE2 Dealing with Issues** section within the QMS.
- **Business Continuity and Disaster Recovery Plans** – are in place so that in the event of a disruption to the information services of the Company, it is possible to activate relevant business contingency plans until affected services are restored.

Policy approved by:

Signed: 31 January 2023



Patrick Evans
Managing Director