Information Security Policy

Introduction

The security and protection of information is fundamental to the effective and efficient working of the Company and the maintenance of confidentiality. This Policy provides a framework within which allows us to handle information and data in the most secure way, given the demands of the service. Security is everyone's responsibility and all personnel working in the Company must make every effort to comply with this Policy.

The company operates a system that regularly evaluates its processes and customer needs and has set quantifiable objectives with plans in place to ensure that they are reviewed year on year for improvement.

The company is committed to continually improving the effectiveness of the information Security management system, and to prevent unauthorized access and use within the company and working environment.

Key Information

The need for the policy

To meet legal and professional requirements and satisfy obligations to our clients, the company must use cost effective security measures to safeguard its information resources. This Company Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The Policy

The Policy of the Company is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised industry best practices that will achieve a balance between cost and risk.

Applicability

The Policy shall apply to all staff of the Company and any other professionals using or interfacing with the IT resources of the Company.

Implementation

The requirements of the Policy shall be implemented by all Directors, staff and other professionals using the Companies IT resources.

Any member of staff noting any area of conflict between this Policy and any other Company Policy must bring it to the attention of the Head of HR, immediately for conflict resolution. Interr, will in any case be responsible for the routine periodic review of the Policy. Staff have an obligation to report suspected breaches of the Policy immediately to Head of HR.

Internal audits will independently review and assess the adequacy of implemented security measures including compliance with the Policy.

Compliance with the Policy is the duty of all Directors and all staff. In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence.

Information Resources

The Policy applies to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by the company. The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

Objectives

The objectives of the Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.
- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

Legal Obligations

General

The Company accepts its obligations to comply with the laws of the United Kingdom and EU. All members of the Company must be aware that there are legal requirements relating to information that must be met.

The principles of these are detailed below:

GDPR and Data Protection Act

Information held electronically that relates to individuals is subject to the Data Protection Act, that places obligations on those who record and use personal data and the organisation for which the work.

The Head of HR is the appointed Data Protection Officer and is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

Software Copyright

Software is protected by the Copyright, Designs and Patents Act 1988, which state that ‘the owner of the copyright has the exclusive right to copy the work’.

It is illegal to make copies of software without the owner’s permission. Penalties include unlimited fines and up to two year in prison.

Computer Misuse Act

The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer.

The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

Company Security Coordinator

CFO is the nominated Security Co-ordinator for the Company and shall:

- Develop and manage the Company security programme.
- Develop, issue and maintain the IT security strategy and Policy
- Develop a strategic IT Disaster Recovery & Service Continuity Plan and advise the Company on its implementation.
- Create an information security awareness programme to include whole Company briefings, training and education.
- Provide information security consulting support to the Company.
- Investigate breaches of security and report findings and recommended action to the Company.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Report annually to management review meeting on the effectiveness of the overall information security programme.

Key Security Controls

Personal Security

- Head of HR will ensure that all contracts of employment include a 'non-disclosure clause/ confidentiality agreement'.
- Head of HR will ensure that security responsibilities are allocated to staff and written into job specifications and terms of reference.
- Security education and training will be provided to all staff as appropriate to their assessed needs.

Physical Security Control

1. Principle

Resources associated with information processing, such as offices, computer equipment, communications media and paper-based records shall be protected from unauthorised access, misuse, damage or theft.

2. Access

- The non-public areas of the Company premises are designated a secure area. Visitors are to be escorted at all times and a record of visits kept.
- In order to prevent unauthorised access during silent hours all offices are locked.

3. Equipment Security

- All hardware and software assets held by the Company are to be held against a hardware register.
- No alteration to the hardware configuration of the system may take place without the permission of CFO. Under no circumstances are modems to be attached to any part of the system.
- Only approved systems engineers will be allowed access to hardware or software and such access are recorded.
- Computer hard discs are not to be removed from the Company premises without the written permission of CFO.

- The disposal of any storage media is subject to specific security control

Internal Security Control

1. Principles

All information shall have an official owner who will be fully accountable for its protection and who will be responsible for:

- Assigning a security classification where appropriate.
- Defining who is authorised to access the information on a need-to-know basis.
- Assessing the risks to the security of the information and the impact of its loss, for both short and long periods.
- Employing suitable measures to reduce risks.
- Ensuring that equipment is only utilised for Company business.
- Ensuring that information is authentic, correct, complete and auditable.
- Ensuring that information is backed up regularly and at a frequency commensurate with its usage and is validated in line with the recommendations laid out in the Application for 'Paperless' status.
- Safeguarding and retaining all Company records.
- Ensuring that information exchange with external organisations within or without the Company does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption.

2. Security Incidents and Reporting

A security incident is defined as any event that could result or has resulted in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.
- An adverse impact, for example:
    - Embarrassment to the Company, Clients and staff.
    - Threat to personal safety or privacy.
    - Legal obligation or penalty.
    - Financial loss.
    - Disruption of activities.
- All incidents or information indicating a suspected or actual breach of security must be reported immediately to the Security Coordinator.
- The types of incidents that can result in a breach of security are many and varied. Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the practice.
- Any unusual incident must be reported to the Security Coordinator who will maintain a record of incidents.
- Any member of staff reporting a breach of security will have unhindered access to the Security Coordinator.

If that member believes the breach is as a result of an action or negligence on the part of any member of Company staff then the member will have access direct to the Security Coordinator.

3. Virus Protection

- A computer virus is a computer program, which 'infects' (modifies or attaches itself to) other computer programs. It then replicates itself and when a set of conditions arises it performs its intended function. This can range from a silly message to the destruction of the complete data holding of a system.
- A constantly running anti-virus software package has been provided and where possible set to auto update latest virus signatures. This does not absolve users from specifically checking any externally sourced disc for viruses before downloading any data or application.

4. Passwords

Passwords are an effective security measure only if they are properly constructed and kept secret. Directors and staff will follow the following routines for password management.

All users should have an individual user name for logon.

- All passwords are to be changed on a regular basis through system forced password changes. Additionally, users are to change their password at any time that they feel their password has been compromised.
- Passwords should be given values that are not associated with personal characteristics, (e.g. children's names, telephone numbers, car registration numbers etc.) Simple and obvious strings of characters and numbers should not be used. It is recommended that a combination of alphabetic, numeric, upper and lower case and system characters be used.
- Passwords should not be written down and are not to be revealed to or shared with other users.

5. System Access Controls

No terminal of PC is to be left logged on and unattended. Users leaving their workstation are to log off the system, or change user, to prevent unauthorised access.

6. Housekeeping

- Data back up of the complete system will be completed daily by IP Integration. All backup data will be accorded the same level of security as live data and held separately at an off-site secure location.
- All software in use by the Company must be licensed and networked applications may be subject to a limited number of users. The Security Coordinator is to ensure that software is correctly used against licences held.
- Software is not to be loaded onto any system or PC without the express authority of the Security Coordinator. This Policy is also to be reflected in employee's terms and conditions of employment.

7. Service Continuity Planning

Disaster Recovery and Service Continuity Contingency plans are produced to ensure the continued fulfilment of the Company mission.

External Security Controls

1. General

Any person not directly a member of the Company is to be considered 'external'.

2. Information Exchange

The exchange of information with, and between, other organisations shall take place within formal arrangements that reflect the legal requirements and the sensitivity of the information.

Staff Compliance

All employed and attached staff must abide by the requirements laid down in this Policy and failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law and/ or a criminal offence

Policy Review

This policy was last reviewed and agreed by the board and seeks to be reviewed and updated as and when required taking into account changing circumstances, legislation, technology and security risks.

Mick Tabori – CEO
March 2020