Information Security Policy

Jan 2017

TABLE OF CONTENTS **PAGE No.**

STATEMENT

The security and protection of information is fundamental to the effective and efficient working of Power System Services 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 practice.

Security is everyone's responsibility and all personnel working in the practice must make every effort to comply with this Policy.

SCOPE OF POLICY

The Need

To meet legal and professional requirements and satisfy our legal obligations, 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 company policy is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised 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 third party using the IT resources of the company.

Implementation

The requirements of the Policy shall be implemented by all staff and other third parties using the companies IT resources.

The company nominated IT security point of contact (Douglas Howie) be responsible for the routine periodic review of the policy.

Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the policy.

Compliance with the Policy is the duty of 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.

Staff have an obligation to report suspected breaches of the policy immediately to IT security POC.

In the case of a breach or suspected breach that could affect the security of Power System Services the IT security POC is to notify the MD without delay.

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 OF THE POLICY

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. All members of the team must be aware that there are legal requirements relating to information that must be met.

The principles of these are detailed below.

Data Protection Act

Information held electronically that relates to individuals is subject to the Data Protection Act 1998, which places obligations on those who record and use personal data and the organisation for which they work.

The IT security POC (Douglas Howie) is 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

KEY SECURITY CONTROLS

Personal Security

- 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**

- 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 an alarm system is provided.

Equipment Security

- All hardware and software assets held by the company are to be held against a hardware register and be uniquely marked as being the property of the practice.
- No alteration to the hardware configuration of the system may take place without the permission of The IT Security POC.
- On-going maintenance arrangements have been agreed with Miller Solutions. A detailed record of faults is recorded on the Miller Solutions System and is to be reviewed at regular intervals.
- Only approved systems engineers (Miller Solutions) staff 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 the IT Security POC
- The disposal of any storage media is subject to specific security control. Simple deletion of files is not adequate and the advice of Miller Solutions is to be requested prior any disposal.

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 utilized 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.
    - 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 IT Security POC (Douglas Howie)
- 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 company.
- Any unusual incident must be reported to IT Security POC who will maintain a record of incidents.
  If an incident is considered to be significant, the Managing Director is to be informed. Any incident where the security of PSS is at risk Miller Solutions is to be notified and the risk assessed.
- Any member of staff reporting a breach of security will have unhindered access to the IT Security POC.

3 System Access Control

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.

4 Service Continuity Planning

Disaster Recovery and Service Continuity Contingency plans are to be produced to ensure the continued fulfilment of the company's task.

POLICY REVIEW

This Policy is to be reviewed on an annual basis by the IT Security POC to take account of changing circumstances, legislation, technology and security risks.

Any revisions to the Policy are to be approved by IT Security POC prior to implementation.

P. Beauchamp: Date: 11th January 2017
Managing Director