# Information Security Policy

**Associated Documentation**

**Legal Frameworks**

- The Data Protection Act (1998)
- The General Data Protection Regulation (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

**Policies**

- Staff Development
- Staff Discipline
- Email Use

**Review & Consultation Process**

Annually from review date. PAS Operations Group to oversee process.

**Responsibility For Implementation & Training**

- Day to day responsibility for implementation: Network Administrator
- Day to day responsibility for training: Training Manager

**Distribution Methods**

This document is made available internally via electronic distribution.

## 1. Introduction

This top-level information security policy is a key component of Personal Audit Systems Ltd's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

The scope of this policy covers all IT resource used in the day to day running of the business, the business's data centre and network environment and all information and technology relating to the provision of managed service to customers. Other organisations, including those providing or receiving services under contracts are subject to this information security policy

We expect that all business partners with access to the businesses information resources to abide by the principles and regulations set out in this policy.

## 2. Objectives, Aim And Scope

2.1. The objectives of the PAS Ltd Information Security Policy are to preserve:
*Confidentiality* – Access to Data shall be confined to those with appropriate authority.
*Integrity* – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
*Availability* – Information shall be available and delivered to the right person, at a time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Personal Audit Systems Ltd by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Personal Audit Systems Ltd or supplied under contract to it.

## 3. Responsibilities For Information Security

3.1. Ultimate responsibility for information security rests with the General Manager of Personal Audit Systems Ltd, but on a day-to-day basis the Network Administrator

shall be responsible for managing and implementing the policy and related procedures.

3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the Operations Group. This review shall take place annually.

3.5. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.6. Each member of staff shall be responsible for the operational security of the information systems they use.

3.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or subcontractors of the external organisation shall comply with all appropriate security policies.

## 4. Legislation

4.1. Personal Audit Systems Ltd is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Personal Audit Systems Ltd, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Personal Audit Systems Ltd shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The General Data Protection Regulation (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

## 5. Policy Framework

*5.1.* *Management of Security*

- At board level, responsibility for Information Security shall reside with the Managing Director.
- The Network Administrator shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation

*5.2.* *Information Security Awareness Training*

Information security awareness training shall be included in the staff induction process.

An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

*5.3.* *Contracts* of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

*5.4.* *Security Control of Assets*

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

*5.5.* *Access Controls*

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

*5.6.* *User Access Controls*

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

*5.7.* *Computer Access Control*

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

*5.8.* *Application Access Control*

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

*5.9.* *Equipment Security*

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

*5.10.* *Computer and Network Procedures*

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the PAS Operations Group.

5.11. *Information Risk Assessment*

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be regularly reviewed feature of Personal Audit Systems Ltd's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. *Information security events and weaknesses*

All information security events and suspected weaknesses are to be reported to the General Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.13. *Classification of Sensitive Information.*

Personal Audit Systems Ltd shall implement appropriate information classifications controls, based upon the results of formal risk assessment to secure their information assets.

The classification of Confidential – shall be used for all client data passing between Personal Audit Systems staff and other organisations under contract.

The classification Restricted -shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

5.14. *Protection from Malicious Software*

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to cooperate fully with this policy. Users shall not install software on the organisation's property without permission from the General Manager. Users breaching this requirement may be subject to disciplinary action.

5.15. *User media*

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Network Administrator before they may be used on Personal Audit Systems Ltd's equipment.

Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

*5.16.* *Monitoring System Access and Use*

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The company has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

*5.17.* *Accreditation of Information Systems*

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the General Manager before they commence operation.

*5.18.* *System Change Control*

Changes to information systems, applications or networks shall be reviewed and approved by the Technical Director and Management Team.

*5.19.* *Property Rights*

The organisation shall ensure that all information products are properly licensed and approved by the General Manager. Users shall not install software on the organisation's property without permission from the General Manager. Users breaching this requirement may be subject to disciplinary action.

*5.20.* *Business Continuity and Disaster Recovery Plans*

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

*5.21.* *Reporting*

The General Manager shall keep the PAS Operations Group informed of the information security status of the organisation by means of regular reports and presentations.

*5.22.* *Policy Audit*

This policy shall be subject to audit by Blue Coffee Networks Ltd.