QMS22– Information Security Policy

Section	Release/Amendment summary	Issue	Date
All	Initial issue	1	28/05/2015
All	Revised	2	19/01/2017
All	Revised to add 4.21	3	02/12/2017
All	Reviewed and amended to include GDPR	4	02/12/2018
All	Reviewed	5	01/01/2019
All	Reviewed / No amend / KK	6	01/11/2020
All	Reviewed- No amends- SM	7	20/7/2021
All	Reviewed	8	19/07/2022
All	Reviewed Kas Khalil	11	21/07/2023
All	Reviewed Kas Khail. Inclusion of reference to BCP and Operational Resilience plan	12	01/07/2024

Approved: Kas Khalil

Management Representative Steve McKeown

Introduction

This top-level information security policy is a key component of Preferred Managements overall information security management framework and should be considered alongside more detailed information security documentation including, system level security mapping (available via Unite), security guidance (available via Unite) and protocols/procedures.

1. Objectives, Aim and Scope

1.1. Objectives

The objectives of the Preferred Management 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 the time when it is needed.

1.2. 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 Preferred Management 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 principals 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.

1.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Preferred Management or supplied under contract to it.

2. Responsibilities for Information Security

2.1. Ultimate responsibility for information security rests with the Managing Director of Preferred Management but on a day-to-day basis all staff shall be responsible for managing and implementing the policy and related procedures.

2.2. All 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

2.3. 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.

2.4. The Information Security Policy shall be maintained, reviewed and updated by the Managing Director or Operations Director. This review shall take place annually, unless required earlier and in accordance with the renewal of required certification.

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

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

2.7. 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.

2.8. 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 sub-contractors of the external organisation shall comply with all appropriate security policies.

3. Legislation

3.1. Preferred Management is obliged to abide by all relevant UK (and international where relevant or deemed applicable) legislation. The requirement to comply with legislation shall be devolved to employees and agents of Preferred Management, who may be held personally accountable for any breaches of information security for which they may be held responsible. Preferred Management shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- 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
- Health & Social Care Act 2001
- General Data Protection Regulation (GDPR) 2018

(list non-exhaustive)

4. Policy Framework

4.1. Management of Security

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

4.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing annual awareness programme is established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality and IT security clause.
- Information security expectations of staff are included within appropriate job definitions.

4.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall be logged against the company asset log (QM03).

4.5. 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.

4.6. User Access Controls

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

4.7. Computer Access Control

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

4.8. 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.

4.9. Computer and Network Procedures

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

4.10. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

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 and at least annually. Any implemented information security arrangements shall also be a regularly reviewed feature of a risk management programme / Management Review. 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.

4.11. Information security events and weaknesses

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

4.12. Classification of Sensitive Information.

A consistent system for the classification of information within Preferred Management enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-Preferred Management controlled bodies.

Preferred Management shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance.

Sensitive information such as financial and contractual records should be marked as Private and Confidential. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or it's employees 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.

Private and Confidential documents should also be stored in lockable cabinets.

4.13. 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 co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Operations Director. Users breaching this requirement may be subject to disciplinary action.

4.14. 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 Operations Director before they may be used on Preferred Management systems. 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. Currently, USB and other removable hard-drives are disabled from all workstations

4.15. 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 via Axis.

Preferred Management 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)
- 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

4.16. 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 Operations Director and Axis Architect before they commence operation.

4.17. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Operations Director and Axis Architect.

4.18. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Operations Director. Users shall not install software on the

organisation's property without permission from the Operations Director. Users breaching this requirement may be subject to disciplinary action.

4.19. 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.

4.20. Reporting

The Operations Director shall keep the Management Team informed of the information security status of the organisation by means of regular reports and presentations.

4.21. Ongoing training

The organisation shall ensure that internal staff are updated of any regulation changes or amendments as well as ongoing training to ensure best practice

5 Related documents

- Purchasing Procedure QMS05
- Control of records procedure QMS02.
- Control of Equipment QMS03
- Asset log
- Auditing Procedure QMS09
- Service Provision and Operations QMS07
- BCP and Operational Resilience plan