Information Security Policy

IS-01

Version 0.3

Version Control

	Last Amended	Author	Action taken
0.1	15/11/2018	Loren Morrison	Document Created
0.2	01/11/2019	Loren Morrison	No amends
0.3	01/11/2020	Kas Khalil	Reviewed – requirement for further review in Q2 of 2021 in line with IT infrastructure changes

Contents

Version Control 2
Contents 3
Information Security Policy 4
Information Security Objectives 4
General Data Protection Regulation (GDPR) 5
Compliance 5
Scope 5
Document Management 5
Exceptions 5
Continual Improvement & Corrective Action Policy 5
This Policy 6

Information Security Policy

This Policy forms the starting point of an overall strategy employed by Preferred Management to ensure the Confidentiality and Integrity of personal, customer and corporate information. This document should not be taken in isolation, but merely provides evidence of our commitment to a robust Information Security Management framework.

As such, Preferred Management are committed to the development and continual improvement of Information Security and Data Protection and the supporting information security management system, in order to provide;

- Assurance with legal, regulatory and contractual obligations
- Reputation management
- Protection of critical assets
- Protection of Personal Identifiable Information (PII) as defined by the Data Protection Act 1998 and the GDPR.

Within Preferred Management, the terms 'Information Security' and 'Data Protection' are intended to describe the same thing, which is the pro-active protection of information/data in all its forms which is under the control of Preferred Management. This document can be referenced as either 'The Data Privacy Policy' or the 'Information Security Policy'

Information is seen as a critical asset of Preferred Management and therefore Preferred Management have developed a set of policies for information security which are approved by management, published and communicated to employees and relevant external parties. These take into account;

- Business strategy;
- Regulatory, legislation and contractual needs; and
- Current and projected information security threats.

Information Security is defined as the *"preservation of confidentiality, integrity and availability of information"*. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved as deemed appropriate to the situation and circumstances.

The core objective of Information Security is to ensure the continuity of service of Preferred Management and minimise the risk of damage by preventing security incidents and managing security threats and vulnerabilities.

Information Security policies are in place to protect Preferred Management's informational assets against internal, external, deliberate or accidental threats and vulnerabilities.

Information Security Objectives

In line with this policy and all supporting information security policies Preferred Management shall ensure that:

- Reduce the risk of information leakages by negligence or human error.
- Ensure Confidentiality, Integrity and Availability of our services and Information held by Preferred Management
- Reduce the risk of security issues from third parties
- Manage the costs associated with Information Security by implementing a structured Information Security Management System (ISMS)

- Reduce the likelihood of a Data breach that will affect our clients, customers, employees and other stakeholders.

General Data Protection Regulation (GDPR)

Preferred Management are committed to the protection of data, both personal and company and see Information Security Management as being the enabler of this. The GDPR, and the six principles within it are of key importance to Preferred Management and it is our intention to ensure that all processes and practices associated to Information Security, are aligned to the GDPR in achieving its aim of reducing the likelihood and/or impact of a data breach on data subjects.

Compliance

Everyone working for Preferred Management has a duty of care for safeguarding the confidentiality, integrity and availability of written, spoken and digital information and are required to comply with this and related Information Security Policies.

All aspects of the security program will be routinely audited to ensure compliance on an annual basis. The objective of this policy is to provide clear direction and support for an information security framework within Preferred Management. This is the primary policy to which all other supporting policy and standards documents are subordinate. This policy will facilitate measurement against and compliance with, ISO27001:2013.

Scope

The policy applies to all permanent, temporary, and contract staff within Preferred Management, and the scope of the ISMS within Preferred Management is outlined within the 'Context and Management System' document.

Where outsourced services are provided to Preferred Management, then reliance is placed upon contractual and legal obligations for the management of information. As a minimum, the service provider is expected to adhere to the Data Protection Act 1998, and GDPR for personal data.

The application of the policy does not apply to clients of Preferred Management, who are expected to have their own Information Security Policy.

Document Management

This document will be made available throughout the business. It will be reviewed for update:

- When specific changes (e.g. organisational, legal, regulatory) have occurred which impact on the policy
- Annually, within 30 days of the anniversary of this document's initial issue
- In response to any concerns raised as to the policy's effectiveness

Exceptions

Exceptions to the Information Security Policy require the written recorded agreement of a member of the SSG.

Continual Improvement & Corrective Action Policy

In order to continually improve the Information Security Management System (ISMS), when a non-conformity occurs Preferred Management will take the following steps;

a) Preferred Management will react to the non-conformity and take appropriate action to control it, correct it, and deal with the consequences as deemed appropriate by the size, scale and nature of the non-conformity.

b) Preferred Management will evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere.

Non-Conformities can be identified in the process of an audit or when an incident occurs. In either situation Preferred Management has committed to a process which will ensure;

1) the non-conformity is assessed;
2) the cause of the nonconformity is determined;
3) an assessment is made of the likelihood that similar non-conformities exist, or could potentially occur;
4) that appropriate actions to rectify are implemented; and
5) effectiveness of any corrective actions taken are subject to review.

Following the identification of a non-conformity and subsequent corrective action plan, the information security management system will be updated when necessary as soon as practicable.

Corrective actions undertaken are always appropriate to the effects of the non-conformities encountered.

Documented information as evidence of corrective actions is maintained, which includes the nature of the non-conformity, any subsequent actions taken, and the results of any corrective action.

This Policy

This document, and the policies within it are subject to ongoing review as part of the annual review cycle and are signed off, annually by the Head of Operations / Operations Director of Preferred Management, who is ultimately accountable for Information Security at Preferred Management.