Information Security Management System (ISMS) Policy

Scope

This policy applies to:

- All Projecting Success employees
- Contractors and Third Parties
- Customers and Clients

Version Control

Author	Version Number	Date	Changes Made
Tallulah Carter-Kelly	1	18/09/2023	Recreated the policy from the previous version created by YS (07/10/2022)

Introduction

Projecting Success provides services and functions which rely on resources including information. The use of information assets must be in line with good professional working practices and procedures as well as statutory, regulatory, and contractual requirements and must ensure the confidentiality, integrity, and availability of all information assets.

Information is an extremely important asset and enables Projecting Success to fulfil its business functions and obligations to clients and customers. ISO/IEC 27001:2013, the international security standard for information security management systems provides mandatory requirements for implementing, reviewing, and continuously improving an Information Security Management System (ISMS).

The Projecting Success ISMS shall ensure the organisation meets its statutory, regulatory, and contractual information security requirements including those provided by the Data Protection Act 2018 and the Information Commissioner's Office (ICO). The ICO is the UK's independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy and security for individuals. To this end, it has imposed fines on public bodies for not protecting information satisfactorily. Further to this, some external partners are only willing to deal with other partner agencies which adhere to high information security standards, and this increasingly means achieving and maintaining ISO 27001 compliance.

Purpose

This policy defines the ISMS policy in terms of the characteristics of the business, the organisation, and its assets. It establishes Projecting Success' principles, ambitions and objectives when utilising a management system for information security.

The scope of this policy relates to use of the O365 environment, databases and computer systems operated by the company in pursuit of the company's business of providing project, programme, portfolio, and data analytics services. It also relates where appropriate to external risk sources including functions which are outsourced.

Policy Statement

This policy defines the ISMS policy in terms of the characteristics of the business, the organisation, and its assets. It establishes Projecting Success' principles, ambitions and objectives when utilising a management system for information security and to maintain an information management system designed to meet the requirements of ISO 27001 in pursuit of its primary objectives, the purpose, and the context of the organisation.

It is the policy of Projecting Success to:

- make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the business management system. For this reason, the policy is displayed on our website to ensure that it's fully accessible.
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities; therefore, as a company, we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.
- train all employees on how to use their own devices, how to make sure the data they are handling is kept secure and any other requirements to enable these objectives to be met. Training will be carried out during onboarding, and then at least once every quarter. The training will include, but is not limited to, staff training presentations, quizzes, external speakers and relevant CPD and will cover all relevant topics related to data security such as GDPR, Cyber Security, Threat Landscapes and best practices.
- ensure that all employees are made aware of their individual obligations in respect of this information security policy.

- maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on “risk”.

This information security policy provides a framework for setting, monitoring, reviewing, and achieving our objectives, programmes, and targets.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by “Top Management” to ensure it remains appropriate and suitable to our business. The Business Management System is subject to both internal and external annual audits.

Last date Reviewed: 18th September 2023

Signed by: Tallulah Carter-Kelly

Role: Information Security Manager