DTP Information Security

Group Policy

Version 1.1

Prepared by: Marcus Muldoon

Date: 14/2/22

SOLVING IT TOGETHER

Document Information

Document Name	DTP Information Security Policy
Brief Description	DTP Group Information Security (ISMS) Policy
Document Author	David Smith
Revision Period	Per Annum

Change History

Version	Date	Changed By	Changes
V0.1	18/6/2021	David Smith	Document Creation
V1.0	21/9/2021	Marcus Muldoon	Minor Revisions
V1.1	14/2/2022	Marcus Muldoon	Minor Revisions & Reformatting

Contents

Information Security Policy

The Directors of DTP Group, which operates as an IT Solutions Provider, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial standing.

DTP Group's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an Information Security Management System (ISMS).

DTP Group is committed to achieving and maintaining certification of its ISMS to ISO 27001:2013 and compliance with the GDPR and the Data Protection Act 2018 (as re-enacted or amended).

Information and information security requirements will continue to be aligned with DTP Group's goals, and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Information Security Manager is responsible for the management and maintenance of the Risk Treatment Plan.

In particular, Business Continuity and contingency plans, data backup procedures, protection from malware and hackers, access control to systems, and information security incident reporting are fundamental to this Policy. Control objectives for each of these areas are supported by specific documented policies and procedures.

DTP Group aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All staff of DTP Group are expected to comply with this Policy and with the ISMS that underpins this Policy. All staff, and certain external parties, will receive appropriate training. The consequences of breaching the Information Security Policy are set out in the organisation's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement. DTP Group has established a top-level management commitment to support the ISMS framework and to review the Information Security Policy periodically and upon significant business change.

In this Policy, Information Security is defined as:

"Preserving the availability, confidentiality, and integrity of the physical (assets) and information assets"

This is expanded on below.

Preserving

This means that management, all full-time or part-time employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All staff will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.

the availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient, and DTP Group must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information. There must be appropriate Business Continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore the prevention of both deliberate and accidental unauthorised access to DTP Group's information, proprietary knowledge, and its systems.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial, or complete, destruction or unauthorised modification of either physical assets or electronic data. There must be appropriate contingency, data backup plans and security incident reporting. DTP Group must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of DTP Group including, but not limited to, buildings, equipment, people, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile

phones and PDAs, as well as on USB sticks or other removable media, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.) of DTP Group.

DTP Group and partners that are part of our integrated network have been made aware of our ISMS.

A current version of this Policy document is available to all members of DTP Group staff and is communicated to all new staff at Induction.

This Policy is reviewed for effectiveness and suitability on at least an annual basis or upon significant business or organisational change. It is issued on a version-controlled basis under the signature of the Group Managing Director.

Name:	Howard Hall
Position:	Group Managing Director
Date:	14 February 2022
Signature: