Information Security Policy

Date of 1st Issue:	30th April 2012
Author:	Paul Horn
Version Number:	9
Last Review:	January 2019
Next review:	January 2020

Table of Contents

DEFINITION

The Company: Refers to Pertemps Network Administration Limited and all of its subsidiary and associated companies.

Policy Statement

Information is a critical asset of The Company. Accurate, timely, relevant, and properly protected information is essential to the success of The Company activities. The Company is committed to ensuring all accesses to, uses of, and processing of information is performed in a secure manner.

This policy and supporting policies and procedures that form The Company Information Security Management System (ISMS) apply to all staff of The Company and all clients and other users authorised by The Company.

The Company is committed to adopting a security model in line with ISO27001 international certification standard and associated best practice guidelines. In addition, it is the intent of The Company to seek verification of its compliance through external certification with a United Kingdom Accreditation Service (UKAS) accredited certification body.

Information systems play a major role in supporting the day-to-day activities of The Company. These information systems include but are not limited to all infrastructure, networks, hardware, software, and paper processes, which are used to manipulate, process, transport or store information used by The Company.

The object of this Information Security Policy is to define the management approach necessary to safeguard The Company's information systems and ensure the security, confidentiality and integrity of the information held therein.

The Policy provides a framework in which security threats to The Company's Information Systems can be identified and managed on a risk basis, and establishes terms of reference which ensure uniform implementation of information security controls throughout The Company.

The Company recognises that failure to implement adequate information security controls, and resulting breaches of information security, could potentially lead to:

- Financial loss
- Irretrievable loss of data
- Damage to the reputation of The Company
- Legal consequences

Therefore, measures must be in place which will minimise the risk to The Company from unauthorised access modification, destruction or disclosure of data, whether accidental or deliberate. This can only be achieved if all staff observes the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and The Company policies, procedures, and technical standards.

The objectives of the Information Security Policy are to:

- Ensure that information is created, used, and maintained in a secure environment.
- Ensure that all of The Company computing facilities, programs, data, network, equipment, and documents are adequately protected against loss, misuse or abuse.

- Ensure that all users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.
- Ensure that all users are aware of and fully comply with the relevant UK legislation, regulation and contractual requirements.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of the ISMS.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the information they handle, in whatever form it make take.
- Ensure that all users have a commitment to satisfy applicable requirements with regards to Information Security and to continually improve the Information Security Management System.

Appropriate Key Performance Indicators (KPIs) will be developed to measure the ongoing effectiveness of the ISMS and help to ensure continual improvement of related security controls.

ISMS Scope

The ISMS and its associated UKAS accredited certification scope is defined as follows:

Information Security Management for the provision of Payroll and ICT services to the Pertemps Network Group Ltd and all of its subsidiary and associated companies.

Location

Meriden Hall, Meriden

Assets and Technology

ESOS information and client information under management control.

All IT systems owned by, or administered by, ESOS

Management of third-parties involved in the provision of IT, hosting or management services.

Exclusions

Non- The Company employees located within Meriden Hall. Where ISMS activities are carried out by these teams, these are captured within an Operating Level Agreement (OLA).