Information Security Policy

Information is a critical asset of Pertemps Network Administration Limited. Accurate, timely, relevant, and properly protected information is essential to the success of Pertemps Network Administration's activities. Pertemps Network Administration Limited 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 Pertemps Network Administration Limited Information Security Management System (ISMS) apply to all staff of Pertemps Network Administration Limited and all clients and other users authorised by Pertemps Network Administration Limited.

Pertemps Network Administration Limited 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 Pertemps Network Administration Limited 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 Pertemps Network Administration Limited. 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 Pertemps Network Administration Limited.

The object of this Information Security Policy is to define the management approach necessary to safeguard Pertemps Network Administration'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 Pertemps Network Administration'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 Pertemps Network Administration Limited.

Pertemps Network Administration Limited 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 Pertemps Network Administration
- Legal consequences

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