Information Security Policy

1 Policy

The aim of this Policy is to ensure the confidentiality, integrity and availability of all information obtained, handled and used by Quest Information Systems Ltd t/a DictateNow.

The following objectives support this policy:

- Provides assurance within the company and to our customers, suppliers, partners, interested parties and other relevant stakeholders that the availability, integrity and confidentiality of their information will be maintained appropriately.
- Manages information security risks to all company and customer assets.
- Protects the company's ongoing ability to meet contracted commitments through appropriate Business Continuity.
- Bases information security decisions and investments on risk assessment of relevant assets considering; Integrity, Availability and Confidentiality.
- Takes into account business and legal or regulatory requirements, and contractual security obligations.
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities.
- Minimises the business impact and deals effectively with security incidents.
- Implements a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001 Standard for Information Security Management Systems.
- Implements a sensitive information control policy including compliance with regulations under the Data Protection Act 1998 to protect customers, suppliers, partners, other relevant stakeholders, our own and personal employee information which is not in the public domain.
- Implements an Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented.
- Develops and implements a Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
- Defines security controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information.
- Provides information security awareness guidance for all company employees.
- Ensures the Management that supports the continuous review and improvement of the company IMS.

- Implements incident management and escalation procedures for reporting and investigation of security incidents for IMS management review and action.

It is a guiding principle that all DictateNow employees are responsible for Information Security.

This Policy will available to interested parties, if relevant and appropriate.

The Policy is supported by the Company's Quality and Information Security objectives.

This Policy us reviewed annually by the Managing Director and may be update as part of continual improvement plan.

Approved by: Garry Park, Managing Director

Date: 30 March 2015