PLANIXS

Information Security Policy

Contents

1 Introduction

This document defines the information security policy of Planixs GRP Limited (Planixs).

As a modern, forward-looking business, Planixs recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Planixs has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

Planixs has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

This policy applies to all systems, people and processes that constitute the Organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Planixs systems.

2 Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within Planixs will be agreed and maintained with the internal business so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Planixs Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Planixs. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following code of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002 – Code of practice for information security controls

The adoption of this code of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual improvement of the ISMS

Planixs policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information security policy areas

Planixs defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the Organisation.

Table 1: Set of policy documents

2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies formally communicated have been reviewed and approved by the top management of Planixs and must be complied with.