Information Security Policy

Contents

Tables

1. Introduction

This document defines the information security policy of Alkath Group.

As a modern, forward-looking business, Alkath Group 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, Alkath Group has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO 27001:2013. 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
- Compliance with legal and regulatory requirements

Alkath Group has decided to maintain full certification to ISO 27001:2013 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body.

This policy applies to all systems, people and processes that constitute the organisation's information systems, including directors, employees, suppliers and other third parties who have access to Alkath Group systems.

2. Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within Alkath Group will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focused 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 Alkath Group 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 27001:2013 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Alkath Group. 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 codes of practice will be adopted and implemented where appropriate:

- ISO 27002:2013 – Code of practice for information security controls
- ISO 27017:2015 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

The adoption of these codes 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

Alkath Group 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 27001:2013 and related standards
- Achieve ISO 27001:2013 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, including cloud service customers
- 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

Alkath Group 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.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties:

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Acceptable Internet Use Policy (P-INS-02)	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Social Media Policy (P-INS-03)	Guidelines for how social media should be used when representing the organisation and when discussing issues relevant to the organisation.	All employees
Cloud Computing Policy (P-INS-04)	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement, Setup and management of cloud services
Mobile Device Policy (P-INS-05)	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organisation or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
BYOD Policy (P-INS-26)	Sets out the controls that must be in place when an employee uses their own mobile device for work tasks.	Users of BYOD (Bring Your Own Device) mobile devices
Teleworking Policy (P-INS-06)	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and employees involved in setting up and maintaining a teleworking site
HR Security Policy (P-INS-07)	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
Acceptable Use Policy (P-INS-08)	Employee commitment to organisational information security policies	All employees
Asset Management Policy (P-INS-09)	This document sets out the rules for how assets must be managed from an information security perspective.	All employees
Access Control Policy (P-INS-10)	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy (P-INS-11)	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy (P-INS-12)	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Clear Desk and Clear Screen Policy (P-INS-13)	Security of information shown on screens, printed out and held on removable media.	All employees

Anti-Malware Policy (P-INS-14)	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organisation's infrastructure from malware
Backup Policy (P-INS-15)	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Logging and Monitoring Policy (P-INS-16)	Settings for event collection. protection and review	Employees responsible for protecting the organisation's infrastructure from attacks
Software Policy (P-INS-17)	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All employees
Technical Vulnerability Management Policy (P-INS-18)	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Employees responsible for protecting the organisation's infrastructure from malware
Network Security Policy (P-INS-19)	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy (P-INS-20)	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Secure Development Policy (P-INS-21)	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships (P-INS-22)	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy (P-INS-23)	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy (P-INS-24)	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Privacy and Personal Data Protection Policy (P-INS-25)	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data

Table 1: Set of policy documents

Details of the latest version number of each of these documents is available from the BMS Summary of Management System Documentation (R-MAN-01).

2.5 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Alkath Group and must be complied with.

Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organisation's Employee Disciplinary Process.

Questions regarding any Alkath Group policy should be addressed in the first instance to the employee's immediate line manager.

....

Phil Guy – Managing Director **Date**