



Altenar Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-05-4
VERSION	1.1
DATED	2024/09/25
DOCUMENT AUTHOR	Denise Vella
DOCUMENT OWNER	Information Security Team

Revision History

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	22/05/2024	Denise Vella	First Version - high level security policy that covers section 5.2 and section 6.2 of ISO 27001:2022
1.1	2024/09/25	Denise Vella	Rebranding

Information Classification

This document is categorised according to the Information Sensitivity Policy.

Classification
☒ Public
☐ Internal
☐ Confidential
☐ Restricted

Approval

NAME	POSITION	SIGNATURE
Stanislav Silin	CEO / CTO	Google drive digital signature
Dinos Stranomitis	COO	Google drive digital signature

Contents

Tables

1 Introduction.....	4
2 Information security policy.....	5
2.1 Information security requirements.....	5
2.2 Framework for setting objectives.....	5
2.2.1 High level Information Security Objectives.....	5
2.3 Information Security roles and responsibilities.....	6
2.4 Continual improvement of the ISMS.....	6
2.5 Information security policy areas.....	7
2.6 Application of information security policy.....	11

1 Introduction

This document defines the information security policy of Altenar. As a modern, forward-looking business, Altenar 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, Altenar 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:

- Information protection against unauthorised access or malicious intent;
- Confidentiality, integrity and availability of information will be maintained;
- Compliance with legal and regulatory requirements
- Continuity plans will be produced, tested and maintained;
- Information security culture.
- Proper handling of security incidents
- Copyright of intellectual property will be respected;

Altenar 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, processes, employees and contractors (herein referred to as "employees") making use of the Altenar information systems. Each employee shall be responsible for maintaining a secure stance in the execution of their duties. The policy is maintained by the information security team and new versions of this policy are approved by management.

The following supporting documents are relevant to this information security policy:

- Statement of Applicability
- Information Security Context, Requirements and Scope
- Information Security Management System Manual
- ISMS Documentation Log
- Altenar Internal Security Policy (which incorporates a number of policies)
- Risk Assessment and Treatment Process
- Incident Response Procedure
- Process for Monitoring, Measurement, Analysis and Evaluation

- Procedure for Internal Audits
- Procedure for Management Reviews

2 Information security policy

2.1 Information security requirements

A clear definition of the requirements for information security within Altenar will be agreed and maintained 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 Altenar 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

Information security objectives will be discussed and set out during the biannual management review meetings. 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 Altenar. 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 controls from the ISO/IEC 27002 – Code of practice for information security controls will be adopted and implemented where appropriate. 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.

2.2.1 High level Information Security Objectives

In line with the standard, it is essential that our information security objectives are consistent with our policies, measurable where practical, communicated effectively within the organisation (and outside where appropriate) and updated as part of the ISMS management review process.

The high level objectives are

- To ensure the confidentiality, integrity and availability of organisation information including all personal data as defined by the GDPR based on good risk management, legal, regulatory and contractual obligations, and business need.
- To provide the resources required to develop, implement, and continually improve the information security management system.
- To effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks.
- To implement a culture of information security and data protection through effective training and awareness.
- To maintain regulatory compliance obligations

2.3 Information Security roles and responsibilities

Information security is the responsibility of everyone to understand and adhere to the policies, follow processes and report suspected or actual breaches. Specific roles and responsibilities for the running of the information security management system are defined and recorded in the document **Information Security Management System Manual**.

2.4 Continual improvement of the ISMS

Altenar 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 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.

2.5 Information security policy areas

Altenar defines policies 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. Some of these policies are documented as a separate document and some are incorporated in the detailed Internal Information Security Policy document. Details of the latest version number of each of these policies is available from the ISMS Documentation Log.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Internet Acceptable Use Policy	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
Employee Device Policy	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
Teleworking Policy	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
Access Control Policy	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	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
Password Policy	Guidance on the security of secret data	All employees
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	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	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	Settings for event collection. protection and review	Employees responsible for protecting the organisation's infrastructure from attacks
Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Employees responsible for protecting the organisation's infrastructure from malware
Server Security Policy	Server security and configuration guidelines	Employees responsible for designing, implementing and managing servers

Network Security Policy	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	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Secure Development Policy	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	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software licence compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media.	All employees
Social Media Policy	Guidelines for how social media should be used when representing the organisation and when discussing issues relevant to the organisation.	All employees

HR Security Policy	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
Acceptable Use Policy	Employee commitment to organisational information security policies	All employees
Policy on Documented Information	Guidelines for the naming, versioning, labelling, approval and publishing of documented information	All employees
Information Sensitivity Policy	Guidances on classification of information assets	All employees
Risk Assessment Policy	Requirements to implement a risk assessment	Asset owners
Incident Response Policy	Requirements for reporting of suspected or real incidents. This policy outlines the expected response mechanism to various types of incident. It also refers to the procedures for identifying, reporting, and categorising security incidents to ensure timely and effective responses	All employees
Asset Management Policy	Covers roles and responsibilities of asset owners	All employees
Availability Management Policy	Covers design, planning and monitoring for availability	Employees responsible for the continuity of business such as infrastructure and monitoring
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All Employees
AI Tools Usage Policy	To establish guidelines and best practices for the responsible and secure use of Artificial Intelligence (AI) tools, specifically focusing on applications like ChatGPT, within our organisation.	All Employees
Change Management Policy	Formal procedures for requesting, reviewing, and approving changes to ensure consistency and minimise risks. It also outlines the roles and responsibilities of stakeholders involved	All employees

	in the change process, including communication and documentation requirements to maintain accountability.	
--	---	--

Table 1: Set of policy documents

2.6 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 Altenar 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 Altenar policy should be addressed in the first instance to the employee's immediate line manager or any member of the security team.