**AlphaTech Information Security  
Objectives and Plan**

|  |  |
| --- | --- |
| DOCUMENT CLASSIFICATION | Confidential |
| DOCUMENT REF | ISMS-DOC-06-1 |
| VERSION | 1 |
| DATED | 28 August 2025 |
| DOCUMENT AUTHOR | Stephanie Uzama |
| DOCUMENT OWNER | Chief Security Officer |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |
| --- | --- |
| NAME | TITLE |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | POSITION | SIGNATURE | DATE |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

**[Tables 3](#_Toc322)**

**[1 Introduction 4](#_Toc11517)**

**[2 Information security objectives 5](#_Toc19508)**

**[3 Plan to achieve objectives 7](#_Toc6083)**

**[4 Resources to manage and improve the ISMS 9](#_Toc18475)**

[4.1 Human resources 9](#_Toc4519)

[4.2 Technical resources 9](#_Toc10568)

[4.3 Information resources 11](#_Toc14740)

[4.4 Financial resources 11](#_Toc10456)

**[5 ISMS risks and opportunities 12](#_Toc18822)**

[5.1 Risks to the ISMS 12](#_Toc28475)

[5.2 Opportunities for the ISMS 13](#_Toc11598)

**[6 Conclusion 14](#_Toc21035)**

**TABLES**

[Table 1 : Information security objectives 6](#_Toc15960)

[Table 2 : Plan to achieve objectives 8](#_Toc26630)

[Table 3 : Human resources required to run the ISMS 9](#_Toc6058)

[Table 4 : Information resources required to run ISMS 1](#_Toc6094)2

[Table 5 : Financial resources required to run ISMS 13](#_Toc4543)

Table 6 : Risks to the ISMS ………………………………………………………………………………………………………….15

Table 7 : Opportunities to the ISMS …………………………………………………………………………………………… 16

# Introduction

Alpha Tech is committed to establishing clear objectives and an effective information security plan to protect its key healthcare technology activities and meet its obligations to interested parties, including customers,healthcare providers, regulators, employees and suppliers.

As part of this commitment, the organization has established an Information Security Management System (ISMS) that complies with the requirements of the ISO/IEC 27001 international standard for information security and will be seeking certification to this standard in the near future.

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

Objectives will be based on a clear understanding of our information security requirements, including those from interested parties, and will consider the results of risk assessments carried out at various levels within the organization.

Alpha Tech’s plan to meet its information security objectives is also described, including:

* What will be done
* What resources will be required
* Who will be responsible
* When it will be completed
* How the results will be evaluated

This document should be read in conjunction with other components of the ISMS, which give background information about internal and external issues relevant to the Alpha Tech’s purpose, the requirements of interested parties and Alpha Tech’s information security policy.

These include:

* *Information Security Context, Requirements and Scope*
* *Information Security Management System Manual*
* *Information Security Roles, Responsibilities and Authorities.*

# Information security objectives

In order to assess whether the ISMS is working as intended it is essential that clear objectives are defined, and a system of monitoring and measurement established to record progress against targets.

High-level objectives for information security are described in the ISMS document *Information Security Context, Requirements and Scope* and the overall framework for setting lower-level objectives is defined in the *Information Security Management System Manual*, also a key component of the ISMS.

Methods for determining to what extent objectives are being met are set out in the document *Process for Monitoring, Measurement, Analysis and Evaluation*.

As part of the ISMS management review process, objectives for information security are regularly set, reviewed and updated in the following major areas:

* Quality – how effectively Alpha Tech’s healthcare information assets including PHI and PII are safeguarded by the ISMS.
* Capability – the knowledge, skills and experience available within the company’s workforce and to some extent externally, to maintain strong security practices.
* Cost – financial resources required to adapt, maintain and improve the ISMS in line with evolving regulatory requirements and cyber threats.
* Resource utilisation – how effectively Alpha Tech employs human, technological and financial resources to maintain security controls.
* Risk reduction – the degree to which known risks are treated to within acceptable limits.
* Other – appropriate objectives that do not fall into any of the above areas.

In discussion with the management team and based upon documented requirements, Alpha Tech has agreed specific objectives in the area of information security as shown in Table 1 below.

Achievement against these objectives will be tracked as part of regular management reviews of the ISMS.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| REF | AREA | OBJECTIVE | MEASUREMENT METHOD | TARGET | TIMESCALE | OBJECTIVE OWNER |
| 1. | Quality | Ensure that all identified ISMS controls are implemented and maintained effectively. | Percentage of identified ISMS controls implemented and validated through internal audit. | 80% | Aug 30 2026 | Information Security Manager |
|  |  | Ensure all business continuity plans have been tested with the last 2 years. | Percentage of plans tested within 2 years | 75% | Aug 20 2026 | Business Continuity Manager |
| 3. | Capability | Training in information security has been provided for all key resources | Number of people trained | 50% | Dec 30 2025 | Information Security Manager |
| 4. | Cost | Optimize information security spending to ensure cost-effective protection without overspending. | Percentage reduction on last year’s budget | 5% | Dec 30 2025 | Information Security Manager |
| 5. | Resource utilisation | Increase number of days provided by business teams for information security activities | Percentage increase over last year’s commitment | 10% | Oct 15 2025 | Chief Operations Officer |
| 6. | Risk reduction | Reduce number of high priority risks on risk register | Number of major ISMS incidents reported per quarter | 10% | Dec 30 2025 | Information Security Manager |
| 7. | Other | All servers have anti-virus installed | Percentage of servers with anti-virus installed | 100% | Sept 20 2025 | Chief Information Officer |

Table 1: Information security objectives

# Plan to achieve objectives

In order to achieve our objectives, it is essential that we have a clear plan that is adequately resourced and has the full support of top management. The success of this plan will determine whether Alpha Tech remains adequately protected against unwanted events and their potential impacts.

The plan is shown in Table 2 below. The tasks required in order to achieve each objective are listed, together with the resources required, person responsible and completion timescale for each one. The method of evaluating the success of each task will vary according to the nature of the task, but an attempt to determine this is also shown.

This plan will be managed in conjunction with background improvement activities, which may be driven by internal and external audit results, risk assessments and management reviews, amongst other sources. Additionally, more detailed plans may also be created in order to control the activities required and take account of internal and external dependencies.

Progress against the plan will be tracked by the Information Security Manager and reported to top management on a regular basis. If a task is looking unlikely to be completed within the target timescale, the effect on the relevant information security objective should be evaluated. Depending on the conclusion, top management may decide whether to act, such as increasing the resources available, to improve the expected completion time.

If information security objectives are changed, the associated plan will also need to be revised.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| REF | OBJECTIVE | TASKS | RESOURCES REQUIRED | PERSON RESPONSIBLE | COMPLETION TIMESCALE | EVALUATION METHOD |
| 1 | Ensure that all identified ISMS controls are implemented and maintained effectively | List controls  Implement controls  Verify controls | Specialist IT team  Internal audit | Information Security Manager | 12 months | List of signed off controls |
| 2 | All business continuity plans have been tested with the last 2 years | Agree testing schedule  Conduct tests  Produce test reports | Operational staff time | Business Continuity Manager | 12 months | Business Continuity test reports |
| 3 | Training in information security has been provided for all key resources | Identify key resources  Identify courses  Attend courses  Complete training records | Training budget  Time of attendees | Information Security Manager | 6 months | Training records |
| 4 | Optimize information security spending to ensure cost-effective protection without overspending. | Review budget  Identify savings  Evaluate effect of reduction | Finance Manager | Information Security Manager | 12 months | Financial budget reports |
| 5 | Increase number of days provided by business teams for information security activities | Agree allocation with top management  Plan involvement  Conduct activities  Record days spent | Business teams | Chief Operations Officer | 12 months | Timesheets of key personnel |
| 6 | Reduce number of high priority risks on risk register | Hold workshops to identify ideas  Implement ideas  Reassess risks | Risk owners  IT team | Information Security Manager | 9 months | Risk register |
| 7 | All servers have anti-virus installed | Identify servers without AV  Install AV and verify | IT specialist | Chief Information Officer | 3 months | Reports from enterprise anti-virus software |

Table 2: Plan to achieve objectives

# Resources to manage and improve the ISMS

In addition to the specific resources required to meet the objectives set out within this document, the following resources will be required on an ongoing basis to manage and improve the ISMS.

## Human resources

The human resources needed for the ISMS are shown in Table 3 below. For more details of the specific responsibilities and authorities of the roles described here, see the document *Information Security Roles, Responsibilities and Authorities*.

|  |  |  |
| --- | --- | --- |
| ISMS ROLE | RESOURCES REQUIRED | COMMENTS |
| Information Security Steering Group | 1 day per quarter for each member | Assuming quarterly meetings |
| Information Security Manager | 1 x Full Time Equivalent | Assumed to be a full-time role |
| Information Asset Owners | 1-3 days per quarter | Depends upon nature and number of assets owned |
| Department Managers | 2 days per annum | Mainly awareness activities and participation in incident investigations |
| IT Technicians | No additional resource | Information security is already part of relevant roles |
| IT Users | 1 day per annum | Attendance at awareness events |

Table 3: Human resources required to run the ISMS

Additional human resources needed includes;

1. Contractors/ Consultants- They are brought in for specialized tasks like penetration testing, cloud security reviews and ISO 27001 certificate preparation.
2. Secondments from business units- Temporary support staff assigned from departments (e.g clinical IT and customer support) to provide process input for ISMS implementation.

## Technical resources

The technical resources and equipments needed for Alpha Tech’s ISMS includes;

1. IT hardware and equipments such as

* Laptops and workstations
* MFA devices
* Secure mobile devices
* Networking equipments(routers, switches and firewalls)
* Printers and scanners
* Backup storage devices

1. Software and applications such as;

* Security Information and Event Management(SIEM)
* Endpoint Protection Platform
* Identity and Access Management(IAM) Tools
* Encryption tools
* Data Loss Prevention(DLP) software
* Vulnerability management tools
* Incident management system
* EHR development and testing platforms

1. Cloud and hosted services such as;

* Cloud service provider(CSP)
* Backup and Disaster Recovery Cloud Service
* Collaboration tools
* Access logging and monitoring tools
* Training and awareness platforms

1. Physical Security resources such as;

* Visitor sign-in system
* Lockable storage cabinets

## Information resources

The Information resources needed for the ISMS are shown in Table 4 below. For more details of the purpose, frequency of use and source.

|  |  |  |  |
| --- | --- | --- | --- |
| **Information Resource** | **Purpose** | **Frequency of Use** | **Source** |
| Audit logs and Monitoring Reports | Detect and analyze security events | Daily | SIEM tools, CSP logs |
| Vulnerability Scan and Pen Test Reports | I dentify and remediate system weaknesses | Quarterly or after major changes | Vulnerability scanners, external auditors |
| Incident Reports and Root Cause Analysis | Document and learn from incidents | As incidents occur | Internal reporting systems |
| Access Control and User Activity Reports | Ensure compliance with least priviledge and segregation of duties | Monthly | IAM systems, HR records |
| Backup and Restore Verification Reports | Confirm disaster recovery capability | Quarterly | Backup systems, DR tests |
| Regulatory and Compliance Guidelines | Align with laws and regulations (HIPAA, GDPR, ISO) | As updates are released | Regulators, ISO, NIST, legal counsel |
| Vendor/CSP Compliance Reports | Verify cloud provider compliance | Annually | AWS, Azure, Google SOC 2/ISO reports |
| Industry Benchmarking Reports | Compare security maturity to peers | Annually | ISACA, ISC2, healthcare associations |
| Policies, Procedures and SoA | Core ISMS documentation | Annually | Internal ISMS documents |
| Risk Assessment and Treatment Plans | Identify and mitigate risks | Annually | Risk management records |
| Training and Awareness Records | Demonstrate staff competence | Quarterly | HR, LMS(learning systems) |
| Supplier Security Evaluation | Ensure supplier compliance | Annually | Supplier questionnaires  Audits |
| Change Management and Config Reports | Track system updates and integrity | Weekly | ITSM systems(ServiceNow, Jira) |
| Capacity and Performance Reports | Monitor system reliability | Monthly | CSP dashboards  Performance tools |
| Customer Feedback and Incident Report | Capture user concerns and service impacts | Ongoing | Helpdesk  Customer portals |

Table 4: Information resources required to run the ISMS

## Financial resources

The financial resources needed for the ISMS are shown in Table 5 below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Financial Resources** | **Purpose** | **When needed** | **Type** | **CapEx/OPeX** |
| Security tools and licences | Initial setup of monitoring, access control and protection | Year 1, during setup and major upgrade | Technology investment | CapEx |
| Training and certification | Build ISMS knowledge and awareness | Year 1(initial), refreshing annually | Training | CapEx(initial)  OpEx(ongoing) |
| Risk assessment and consultancy fees | Gap analysis and expert ISMS setup support | Year 1(implementation) | Consulting | CapEx |
| Certification and surveillance audits | ISO 27001 compliance and certification maintenance | Year 1(certification) and annually(surveillance) | Compliance | OpEx |
| Cloud services | Continuous monitoring and resilience | Monthly / Annually ongoing | IT services | OpEx |
| Staff awareness and phishing training | Reduce human risk and improve security culture | Quarterly / Annually ongoing | Training | OpEx |
| Penetration testing and vulnerability scans | Identify and remediate weaknesses | Annually / after major system changes | Testing | OpEx |
| Threat intelligence and IR retainers | Stay ahead of cyber threats and ensure incident response readiness | Ongoing | Security service | OpEx |
| Cybersecurity insurance premiums | Financial protection in case of breaches | Annually | Insurance | OpEx |
| Incident costs | Cover emergency cost | During unexpected incidents | Reserve fund | OpEx |
| Future scalability budget | Expand ISMS as Alpha Tech grows or regualtions change | During new projects/clients | Growth investment | CapEx / OpEx |

Table 5: Financial resources required to run the ISMS.

# 

# ISMS risks and opportunities

## Risks to the ISMS

The following risks have been identified to the effectiveness of the ISMS. These will be managed and updated as part of regular management reviews and the effectiveness of the treatment actions evaluated over time.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REF | RISK | RISK OWNER | LIKE- LIHOOD | IMPACT | SCORE | RISK LEVEL | TREATMENT ACTIONS | TIMESCALE |
| 1 | Resources may not be available to take on the proactive elements of information security management that are not currently being carried out. | ISMS Manager | 3 | 4 | 12 | High | Secure budget approval  Prioritize resources  Escalate to the management during reviews | 3 months |
| 2 | Staff fail to engage with the ISMS leading to issues with the implementation of controls | ISMS Manager | 4 | 4 | 16 | High | Conduct mandatory awareness training  Monitor compliance  Enforce disciplinary measures | Ongoing, reviewed quarterly |
| 3 | Management are not sufficiently involved in the creation of the new management system to carry it forward once certification gained | Board | 2 | 5 | 10 | Medium | Schedule regular management reviews  Assign KPIs for leadership | 6 months |
| 4 | ISMS documentation are not being kept to date thereby causing confusion and compliance gaps. | ISMS Manager | 3 | 3 | 9 | Medium | Establish document control process  Assign document owners | 2 months |
| 5 | Risk assessments are not being carried out consistently or at the required intervals. | Risk & Compliance officer | 3 | 4 | 12 | High | Annual risk assessment schedule  Automated reminders  Assign responsibilty | 1 month |
| 6 | Skipping, delaying and poor execution of internal audits leading to uncontrolled impacts | Internal Auditor | 2 | 4 | 8 | Medium | Establish annual audit plan  Management oversight | 6 months |
| 7 | Suppliers or cloud service providers fail to meet the company’s ISMS requirements. | Supplier Management Lead | 3 | 4 | 12 | High | Enforce supplier security clauses  Periodic audits of suppliers | 6 months |
| 8 | Controls are not being monitored effectively this means that security weaknesses could go undetected | Security Operation Lead | 2 | 4 | 8 | Medium | Deploy monitoring tools  Regular reporting dashboards | 4 months |

Table 6: Risks to the ISMS

## Opportunities for the ISMS

The following opportunities have been identified which may assist in preventing or reducing undesired effects or achieving continual improvement within the ISMS:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| REF | OPPORTUNITY | OPPORTUNITY OWNER | POTENTIAL BENEFIT | ACTIONS | TIMESCALE |
| 1 | Recent security breaches at competitor organizations have raised the profile of information security in the industry | Information Security Manager | May make it easier to convince management of the need for additional controls | Identify controls that may have prevented the breaches at competitors | 3 months |
| 2 | Stricter enforcement of HIPAA, HITECH and state data privacy laws offers an opportunity for Alpha Tech to differentiate itself through compliance | Compliance Officer | Would ensure the avoidance of penalities and create a strong compliance reputation | Map controls to regulations and maintain a legal watch | Ongoing  (annual review) |
| 3 | Cloud service providers now offer advanced tools that Alpha Tech can leverage to strengthen ISMS without heavy in-house investments | Information Security Manager | Ensure scalable security and enhanced protection | Leverage CSP tools and integrate them into ISMS | 6 months |
| 4 | The ISMS framework provides opportunities to improve communication between IT, HR, legal and clinical teams by strengthening goverance and culture. | Information Security Manager | Brings about stronger governance and establishes a better communication | Holding quarterly ISMS cross-department meetings | Quartely |

Table 7: Opportunities for the ISMS

# Conclusion

The objectives defined within this document are critical to defining the core purpose of the ISMS and measuring its success. These objectives provide a clear answer to the question of why business resources need to be allocated to the area of information security and so go some way toward justifying the budget requested.

The objectives set for the period under consideration are intended to be challenging but achievable and will go a long way to protecting the organization from security incidents that may occur both now and in the future.

The creation of a plan to achieve these objectives is an essential part of the continual improvement of the ISMS within Alpha Tech. Taken in conjunction with the internal audit and management review processes, this should help to ensure that we have in place an effective mechanism for managing information security in the longer term.