ALPHA-TECH Information Security Context, Requirements and Scope

|  |  |
| --- | --- |
| DOCUMENT CLASSIFICATION | Confidential- ISO/IEC 27001 Clause 4 Documentation |
| DOCUMENT REF | ISMS-DOC-04-1 |
| VERSION | 1 |
| DATED | 13/8/2025 |
| DOCUMENT AUTHOR | Stephanie Uzama |
| DOCUMENT OWNER | Information Security Manager |

[1. Introduction 3](#_Toc10744)

[2. Organizational context 4](#_Toc23816)

[2.1 Organizational Profile 4](#_Toc13356)

[2.2 Company’s Activities 4](#_Toc5042)

[2.3 Company’s Department 5](#_Toc25724)

[2.4 Company’s core functions 6](#_Toc2430)

[Cloud Services Provided 6](#_Toc25608)

[2.4 Products and services 7](#_Toc2219)

[2.4.1 Products 7](#_Toc2861)

[2.4.2 Services 7](#_Toc19156)

[2.4.3 Alpha Tech Products & Services Analysis 7](#_Toc11525)

[2.5 Supply Chain 8](#_Toc32497)

[3.0 Internal and External Issues 9](#_Toc19430)

[3.1 Internal Issues 9](#_Toc22606)

[3.2 External Issues 10](#_Toc26349)

[3.3 Risk Appetite 10](#_Toc13942)

[4.0 Interested Parties and their requirements 11](#_Toc20700)

[4.1 Interested Parties 11](#_Toc13593)

[4.2 Interested Party - Detailed Register 12](#_Toc17096)

[4.3 Requirements 13](#_Toc11380)

[5.0 Purpose and Scope Of The ISMS 15](#_Toc12661)

[5.1 Purpose 15](#_Toc11729)

[5.2 Potential Impact of an Information Security Incident 15](#_Toc25168)

[5.3 Information Security Objectives 16](#_Toc9484)

[5.4 Scope Of the ISMS 16](#_Toc25950)

### Figures

Figure 1: Organizational chart…………………………………………………………………………………….5

Tables

Table 1: Alpha tech service and product analysis summary……………………………..8

**Table 2: Detailed summary of interested parties……………………………………………..13**

**Table 3: Required summary of interested parties…………………………………………….14**

# Introduction

Alpha Tech is committed to protecting the security of its business information, including Protected Health Information (PHI) and Personally Identifiable Information (PII), in the face of incidents and unwanted events. The company has implemented an Information Security Management System (ISMS) that is compliant with ISO/IEC 27001, the international standard for information security.

The purpose of this document is to describe the way Alpha Tech operates, outline internal and external factors influencing the business, and highlight in general terms the potential consequences of a security breach. This will allow the most appropriate mix of control measures to be implemented to reduce the level of risk and ensure that plans are available and tested to manage the impact of any interruptions that may occur.

Specifically, this document sets out:

* The context of the organization.
* External and internal issues relevant to the purpose of Alpha Tech.
* Interested parties relevant to the ISMS.
* Information security requirements of these interested parties.
* The scope of the ISMS, including its boundaries and applicability.

This document will be reviewed and updated at least annually, or when significant changes occur in the relevant areas covered.

# Organizational context

The organizational context of Alpha-Tech is set out in the following sections. Given the fast-moving nature of the business and the markets in which it operates the context will change over time. This document will be reviewed on an annual basis and any significant changes incorporated. The ISMS will also be updated to cater for the implications of such changes.

## **Organizational Profile**

**Company Name:** Alpha Tech

**Founded**: 2017

**Headquarters & Only Location:** Austin, Texas, USA.

**Business Type:** Private, mid-sized enterprise.

**Main Industrial Sector:** Health Technology (Healthcare IT Solutions)

**Annual Turnover:** Approx. **USD 22 million**

## **Company’s Activities**

The core activities of Alpha Tech includes;

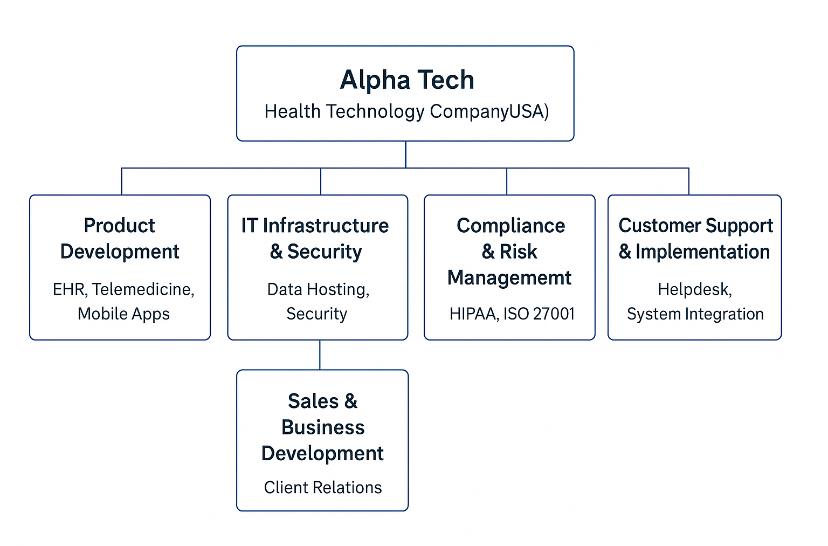
* Product development
* Medical device integration
* Data analytics and AI solutions
* Data management and security
* Compliance and regulatory support
* Customer support and technical assistance.
* Integration and interoperability
* Business contunuity and disaster recovery

## **Company’s Department**

Alpha Tech consists of the following departments;

* Executive management
* Human Resources (HR)
* Finance and administration
* Sales and marketing
* Software Engineering and IT Operations
* Cybersecurity and compliance
* Customer Support and Training
* Research and Development

Alpha Tech organization chart is shown below;

*Figure 1: Organization chart*

## **2.4 Company’s core functions**

* **Healthcare Software Development –** Designing new health technology solutions (EHR systems, patient portals, telemedicine platforms) to meet emerging healthcare needs.
* **Medical Device Integration –** Connecting IoT medical equipment to centralized hospital systems. Deploying software and devices into client environments with minimal disruption.
* **Healthcare Data Analytics & AI –** Predictive analysis, clinical decision support, and population health management.
* **Cybersecurity Solutions for Healthcare –** Ensuring HIPAA compliance, encryption, identity and access management. Protecting patient data and company intellectual property.
* **Customer Training & Support –** Onboarding, user training, and 24/7 technical support as well as customer relationship management.
* **Regulatory Compliance Management –** Ensuring all products meet U.S. healthcare regulations, including HIPAA, FDA, and state-level requirements.
* **Business Development & Sales –** Expanding market presence through strategic partnerships and outreach.

### **Cloud Services Provided**

Alpha Tech offers cloud-based healthcare solutions hosted on secure HIPAA-compliant platforms including;

* Data hosting and backup services
* Software-as-a-service(SaaS)- A subscription based telemedicine platform.
* Platform-as-a-service(PaaS)- A secure API and development environment for hospital system integration.

## **Products and services**

### **2.4.1 Products**

1. Telemedicine platform
2. Electronic Health Record System
3. Mobile Health Apps
4. API Integration suite
5. Healthcare Data Analytics tool

### **2.4.2 Services**

1. 24/7 Technical support
2. Training and User Education
3. Customizing and Installing EHR and telemedicine systems for hospitals and clinics.
4. Systems security and risk management.
5. Compliance Consulting
6. Data backup and diaster recovery.

### **2.4.3 Alpha Tech Products & Services Analysis**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Product/Service** | **Customer’s availability** | **Revenue/ Profit** | **High Profile** | **Regulations** | **Dependencies/ prerequisites** | **Health & Safety Aspect** |
| **EHR Platform** | Offered to hospitals, clinics and research institutions. | High revenue, stable profit | Yes | HIPAA, HITECH, FDA | Requires IT infrastructure and secure hosting. | Direct impact on the accuracy of patient care. |
| **Medical Device Integration** | Hospitals and large clinics. | Moderate revenue, high profit | Medium | HIPAA, FDA | Requires medical devices and infrastructure. | Directly affects patient monitoring and treatment. |
| **Telemedicine Application** | Healthcare providers | Moderate revenue, high profit | Yes | HIPAA, HITECH , State telehealth laws | Requires EHR integration | Affects remote diagnosis and treatment |
| **Healthcare Data Analytics and AI** | Research institutions | Premium, high margin service | Yes | HIPAA, HITECH | Requires access to historical patient data. | Used for predictive diagnosis and treatment recommendations. |
| **Cloud Hosting for healthcare apps** | All existing clients | High revenue, moderate profit | Medium | HIPAA, SOC 2 Compliance | Requires existing Alpha Tech products. | Supports critical healthcare systems |
| **Cybersecurity services** | All existing clients | Moderate revenue, high value to clients. | Medium | HIPAA, NIST | Requires Alpha Tech system usage. | Protect against breaches that could harm patients. |

*Table 1: Alpha Tech Products and services analysis summary.*

**NB:** All EHR, telemedicine and analytics solutions processes protected health information which includes sensitive PII such as patient names, contact details, medical history, diagnoses and treatment plans.

## **Supply Chain**

Alpha Tech’s operations rely on a network of carefully selected suppliers and partners, all based in the United States to maintain HIPAA compliance and avoid risks. They include;

1. **Cloud Infrastructure and Hosting (AWS & AZURE)-**  Alpha Tech's EHR platform, telemedicine app, and analytics services run on HIPAA-compliant cloud environments. This partnership is crucial, generating 70% of revenue. To minimize downtime risks, they use multi-region redundancy.

**2. Medical Device Allies (GE Healthcare, Philips)**: Alpha Tech integrates FDA-approved devices from these partners into their platform. This collaboration enables seamless connections between monitoring devices and patient records, contributing 25% to revenue.

**3. Software Development Essentials (GitHub, Atlassian)**: These tools are vital for Alpha Tech's digital services. They ensure all providers meet HIPAA and SOC 2 standards. The revenue impact is indirect.

4. **Cybersecurity Vendors**: Alpha Tech partners with U.S.-based MSSPs and security software vendors to safeguard services. Vendor compliance with HIPAA and internal security audits are non-negotiable.

**5. Data Protection Specialists :** Long-standing partnerships with DRaaS providers ensure data protection and business continuity, supporting HIPAA and state-specific regulations.

**6. Telecom and Internet providers :** Alpha Tech maintains long-term contracts with internet service providers for stable network connectivity, crucial for telemedicine and cloud-based solutions.

**7. Training & Support Services**: A hybrid model of in-house specialists and U.S.-based training consultants delivers implementation, onboarding, and compliance training, boosting customer retention and satisfaction.

**The Bottom Line:**

- Cloud infrastructure is Alpha Tech's most critical supply chain link.

- Well-established partnerships (many over 5 years) and annual risk assessments ensure service quality.

- Contractual SLAs are in place to guarantee high standards.

# 3.0 Internal and External Issues

There are a number of internal and external issues that are relevant to the purpose of Alpha Tech and that affect the ability of the ISMS to achieve its intended outcome.

### **3.1 Internal Issues**

These includes;

**STRENGTHS**

* Adopted standards and models
* Contractual relationships
* Resources and knowledge
* Company culture

**WEAKNESSES**

* Company financial performance
* Location and physical resilience
* Adopted standards and models
* Operational efficiency
* Third-party dependency
* Increased exposure to cyber threats due to distributed access by remote workers.

### **3.2 External Issues**

They include;

* Cybersecurity threat landscape
* Regulatory compliance burden
* Supply chain risks
* Competitive pressure
* Market demand shifts
* Technological advances
* Reputation risk
* Public health policies
* Geopolitical and legal factors

## **3.3 Risk Appetite**

The ISMS is designed to address the major risks that are identified to the information security of Alpha Tech. In identifying, assessing, and managing these risks, there are several options open to the organization according to its appetite for risk.

In general terms, the organization’s appetite for risk may be said to be Low.

The strategy of the organization is to avoid risk where possible and to invest resources in mitigating residual risk through effective information security measures. This is due to the highly sensitive nature of the data handled (including Protected Health Information and Personally Identifiable Information), the strict regulatory environment (HIPAA, HITECH, and CCPA), and the severe reputational and operational consequences of a security breach in the healthcare sector.

Remote work introduces additional risks for PHI and PII and Alpha Tech maintains a low risk appetite for insecure remote connections.

This general level of risk appetite will be applied to the risk assessments that are carried out as part of the ISMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

The criteria for assessing risk in the context of the organization’s appetite for risk are defined in a separate ISMS document Risk Assessment and Treatment Process.

# 4.0 Interested Parties and their requirements

This section of the document sets out the interested parties that are relevant to the ISMS and their requirements. It also summaries the applicable legal and regulatory requirements to which the company subscribes.

### 4.1 **Interested Parties**

An interested party is a person or organization that can affect, be affected by, or percieve themselves to be affected by a decision or activity. The interested parties relevant to the ISMS includes;

* Hospitals and healthcare providers
* Patient/ end users
* Employees and contractors( Onsite and Remote Workers)
* Shareholders/ investors
* Regulatory authorities
* Business partners and vendors
* Insurance providers
* Industry associations
* Law enforcement and cybersecurity agencies.

Applicable legal and regulatory requirements arise from the following;

* HIPAA (Health Insurance Portability and Accountabilty Act)
* HITECH (Health Information Technology for Economic and Clinical Health Act)
* State- Specific Health Privacy Laws
* CCPA (California Consumer Privacy Act)
* Contractual Obligations
* ISO/IEC 27001:2022

### 4.2 Interested Party - Detailed Register

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Interested Party** | **Nature of Interest** | **Degree of Influence over Alpha Tech** | **Value of the Interest** | **Other Relevant Information** |
| Customers/ Healthcare providers (Hospitals, clinics, private practices) | Depend on Alpha Tech’s EHR and telehealth platforms for patient care. | High | High- Primary source of revenue | Long term service contracts with SLA requirements. |
| Patients/ Endusers | Expect confidentiality, integity and timely access to PHI. | Medium | High- Reputation and compliance risk if dissatisfied. | Protected under HIPAA and state privacy laws |
| Employees (all departments) | Need secure systems stable jobs and a safe workplace. | Medium | High- Core assets are skills and expertise. | Regular security training and efficient teamwork. |
| Regulatory Authorities (HHS, OCR, state health departments) | Enforce compliance with healthcare data protection laws. | High | High- Non-compliance can cause major financial and reputational damage. | Subject to regular auduts and breach reporting requirement. |
| Business Partners / vendors (Cloud service providers, software developers) | Require secure data exchange and integration. | Medium | Medium- Enable core service delivery. | Managed through Business Associate agreements(BAAs) and vendor risk assessment. |
| Investors/Shareholders | Seek profitablity, stability and growth | High | High- Fund ongoing projects and expansions | Require regular governance and financial performance reporting. |
| Insurance Providers(Cybersecurity and liability insurers) | Require evidence of strong risk controls. | Low | Medium- Provide financial protection in case of incidents. | Premium rates tied to Alpha Tech’s security posture. |
| Suppliers( IT hardware and infrastructure providers) | Depends on procurement contracts. | Low | Medium - Impact on operational continuity. | Must comply with Alpha Tech’s supplier security standards. |

*Table 2: Detailed summary of interested parties.*

### **4.3 Requirements**

For details of how applicable legal, regulatory and contractual requirements are identified, accessed and assessed see the ISMS document Legal, Regulatory and Contractual Requirements Procedure. The applicable requirements of interested parties and legal and regulatory bodies are summarised in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S/N** | **Details of Interested Parties** | **Interested Parties Requirement Expectation** | **Source/ Supporting document** | **Requirement met by the ISMS?** |
| 1 | Customers/ Healthcare providers | Secure and reliable health platforms and EHR. | HIPAA  Customer contracts | Yes, by securing EHR systems and enforcing HIPAA compliance. |
| 2 | Patients | Confidentiality, integrity and availability to PHI. | HIPAA  Security rules | Yes, by protecting PHI and managing access controls. |
| 3 | Employees (On-site staff and remote workers) | Secure IT systems  Data privacy protection  Secure remote access to systems, reliable VPN and MFA. | HR Policies  Employment contracts  Remote Work Policy  NIST Guidelines on Telework security  Information security | Yes, by securing internal systems, raising security awareness and protecting staff personal data. |
| 4 | Regulatory Authorities | Compliance with HIPAA and HITECH  Risk assessment | HIPAA  HITECH  State Data Protection Laws | Yes, by maintaing compliance evidence and enabling regular risk assessments. |
| 5 | Business Partners/ Vendors | Secure integration | Vendor Security Management | Yes, by enforcing secure integrations, BAAs and vendor risk management. |
| 6 | Insurance providers | Evidence of strong controls | Cybersecurity Insurance Policy Terms | No |
| 7 | Investors/ Shareholders | Business stability  Strong governance | Corporate Governance Polices | Yes, by avoiding breaches and reputational damage. |
| 8 | Suppliers | Protection of supplier data | Supplier contracts and procurement policy | No |

*Table 2: Requirements summary of interested parties.*

## **5.0 Purpose and Scope Of The ISMS**

### **5.1 Purpose**

1. Understand Alpha Tech’s operational needs in the healthcare technology sector and the necessity for establishing information security management policies and objectives to protect Protected Health Information (PHI) and Personally Identifiable Information (PII).

2. Implement and operate controls and measures for managing Alpha Tech’s capability to prevent, detect, and respond to information security incidents.

3. Monitor and review the performance and effectiveness of the ISMS to ensure ongoing protection of sensitive healthcare data and critical systems.

4. Continually improve Alpha Tech’s information security posture based on objective measurement and evolving threat landscapes.

This purpose applies to the scope of the ISMS as defined below.

### **5.2 Potential Impact of an Information Security Incident**

An information security incident at Alpha Tech could have significant operational, legal, financial, and reputational consequences due to the sensitive nature of healthcare data and the reliance of healthcare providers on our systems. Possible impacts include:

1. Confidentiality Breach of Patient Health Information (PHI)

Unauthorized disclosure of PHI could lead to HIPAA violations, resulting in regulatory fines, lawsuits, and loss of trust from patients and healthcare partners.

1. Operational Disruption

Downtime in the Electronic Health Record (EHR) or telehealth platforms could disrupt clinical workflows, delay patient care, and impact critical healthcare decisions.

3. Financial Loss

Incident recovery costs, legal fees, regulatory penalties, compensation to affected individuals, and potential loss of business contracts.

4. Reputational Damage

Public perception of Alpha Tech’s ability to safeguard sensitive health information could be damaged, leading to reduced market share and difficulty acquiring new customers.

5. Regulatory Non-Compliance

Failure to meet HIPAA, HITECH, and state-level data protection requirements could result in sanctions, audits, and long-term compliance monitoring.

6. Loss of Competitive Advantage

Exposure of proprietary software code, AI algorithms, or product development plans could benefit competitors and undermine Alpha Tech’s market position.

7. Legal Liabilities

Class-action lawsuits from patients or contractual disputes with partners due to breach of service-level agreements (SLAs).

8. Supply Chain Disruption

If an incident impacts vendor systems (e.g., cloud hosting provider breach), Alpha Tech’s ability to deliver services may be delayed or impaired.

### **5.3 Information Security Objectives**

Objective 1 – Comply with applicable healthcare and data protection legislation at all times.

Objective 2 – Protect Protected Health Information (PHI) and Personally Identifiable Information (PII).

Objective 3 – Maintain uninterrupted availability of critical healthcare technology services.

Objective 4 – Preserve Alpha Tech’s reputation and customer trust.

Objective 5 – Minimize financial losses associated with information security incidents.

Objective 6 – Ensure timely detection and response to information security threats.

Objective 7 – Support continual improvement of security practices.

The success of the ISMS will be judged on its ability to meet these overall objectives.

### **5.4 Scope Of the ISMS**

The defined scope of Alpha Tech’s ISMS considers the internal and external issues referred to in sections 3.1 and 3.2 of this document, the requirements referred to in section 4.3. It also reflects the needs of interested parties and the legal and regulatory requirements that are applicable to the organization.

The scope is defined below in terms of the parts of the organization, products and services and related activities.

#### 5.4.1 Organizational

The ISMS applies to Alpha Tech, headquartered in Austin, Texas, USA, covering all business functions, departments, contractors, employees, authorized remote workers involved in the development, provision, and support of healthcare technology products and services.

This includes:

* Software Development Department
* Cloud Infrastructure & IT Operations Department
* Customer Support & Training Department
* Sales & Marketing Department
* Compliance & Risk Management Department
* Human Resources Department
* Executive Management

The ISMS also includes oversight of outsourced services (e.g., cloud hosting, payment processing, and IT security monitoring) where Alpha Tech retains contractual and operational control over security requirements.

#### 5.4.2 Products and Services

The following product and service categories are within the scope of the ISMS:

* Healthcare Software Solutions – Electronic Health Records (EHR) platforms, telemedicine applications and patient data management tools.
* Cloud-Based Healthcare Services – Secure hosting and storage of PHI and PII on Alpha Tech-managed cloud infrastructure.
* Data Analytics & Reporting Tools – Solutions for healthcare providers to gain insights into patient outcomes and operational performance.
* Cybersecurity Services for Healthcare Clients – PHI protection solutions, security monitoring and incident response.
* Technical Support & Training Services – User onboarding, troubleshooting and product education for healthcare providers.

#### 5.4.3 Activities

The following business activities are within the scope of the ISMS:

* Design, development, testing, and deployment of healthcare software solutions.
* Remote access to the company systems by authorized personel, including the use of secure VPNs, MFA and encryption protocols for remote workers.
* Secure hosting and management of cloud-based healthcare systems.
* Processing, storage, and transmission of PHI and PII in compliance with HIPAA and related regulations.
* Provision of customer support and training for healthcare software products.
* Management of third-party vendors involved in healthcare data processing.
* Internal governance, compliance monitoring and continual improvement of information security measures.

#### 5.4.4 Exclusions

The following areas are excluded from the scope of the ISMS:

* Physical building maintenance (e.g. janitorial services, property repairs), as they do not directly impact information security.
* Personal IT devices not used for company operations (e.g. employee-owned devices for personal use).
* Legacy software products no longer supported by Alpha Tech, as they are fully decommissioned and not in active use.

These exclusions do not compromise Alpha Tech’s ability to meet ISMS objectives or deliver secure healthcare technology services.

Version 1 13/8/2025