Information Security Policy in Compliance with ISO 27001 for Clinitalk consultation recording software

**Change control**

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer | Date | Comments | Version |
| N.Boeckx | 25/9/23 | Info security policy review | 1.0 |
| N.Boeckx | 1/4/24 | Info security policy review | 1.1 |
| N.Boeckx | 11/04/2025 | Info security policy review | 1.2 |
|  |  |  |  |
|  |  |  |  |

Next review date: April 2026

Contents

[Introduction 2](#_Toc148423588)

[Purpose 2](#_Toc148423589)

[Clinitalk Information Security Policy Statement (ISO 27001 section 4.1) 2](#_Toc148423590)

[Clinitalk Information Security Policy Summary: 3](#_Toc148423591)

[Assessment of Internal and External Issues Impacting Business Objectives 3](#_Toc148423592)

[Interested parties and requirements (ISO 27001 section 4.2a and b) 5](#_Toc148423593)

[Scope (ISO 27001 section 4.3) 5](#_Toc148423594)

[Responsibilities 5](#_Toc148423595)

[The Clinitalk Board 5](#_Toc148423596)

[Caldicott Guardian 6](#_Toc148423597)

[Senior Information Risk Officer 6](#_Toc148423598)

[Data Protection Officer 6](#_Toc148423599)

[Policy Statements 6](#_Toc148423600)

[Governance 6](#_Toc148423601)

[Asset Management 6](#_Toc148423602)

[Access Control 6](#_Toc148423603)

[Cryptography 7](#_Toc148423604)

[Physical and Environmental Security 7](#_Toc148423605)

[IT Security 7](#_Toc148423606)

[Cloud Security 8](#_Toc148423607)

[Asset and Data Security 8](#_Toc148423608)

[Systems Acquisition, Development and Maintenance 8](#_Toc148423609)

[Risk Management 9](#_Toc148423610)

[Third Party Risk Management 9](#_Toc148423611)

[Information Security Incident Management 9](#_Toc148423612)

[Personnel Security 9](#_Toc148423613)

[Business Continuity 9](#_Toc148423614)

[Compliance 10](#_Toc148423615)

[Policy Compliance 10](#_Toc148423616)

[Non-compliance 10](#_Toc148423617)

[Policy Endorsement 10](#_Toc148423618)

[Overarching principles 11](#_Toc148423619)

[Information Classification 11](#_Toc148423620)

[4. Information Security Management System (ISMS) 11](#_Toc148423621)

# Introduction

Our information security policy outlines our overarching principles, goals and objectives relating to information security.

# Purpose

The purpose of the Information Security Policy is to explain how we apply our information security framework and describes our approach to the protection of the information assets we hold and the services we provide through maintaining appropriate technical, organisational, and physical controls.

# Clinitalk Information Security Policy Statement (ISO 27001 section 4.1)

Clinitalk utilises information assets daily and they are core to our business. Our assets include medical information belonging to customers which may contain sensitive personally identifiable information (PII) and which therefore requires protection and confidential classification. We manage a cloud service, hardware, servers, systems, and staff. It is vitally important (to our customers and to us as an organisation) that we ensure that these information assets are subject to adequate and appropriate safeguards against any unauthorised or unlawful use or disclosure, and that we ensure that we are complying with all applicable legal, regulatory, and contractual requirements. Clinitalk uses a risk based approach to manage information security risks appropriately. This framework is designed to meet the international standard ISO 27001:2013.

By establishing an organisation-wide approach to information security, we will:

* Reduce the risk of our information security systems and processes being compromised to an

appropriate level as defined by the Business

* Prevent the misuse of any information assets we hold (both our own and that which we hold

on behalf of our customers and employees)

* Ensure the company satisfies all its legal, regulatory, contractual and ethical responsibilities with regards to its handling of sensitive and confidential data
* Have an effective process for responding to information security incidents
* Have an effective process to respond to any real or perceived non-compliance with any applicable information security policies and procedures
* Define the process for measuring the effectiveness of Clinitalk information security policies
* Communicate the information security framework and underlying principles to new and existing employees, agents, contractors, partners and third parties by way of regular reminders and training sessions
* Ensure processes and procedures enabling employees to raise security concerns are effective and meet Business needs
* Engender a culture within Clinitalk that recognises the value and importance of information security so that everyone that is part of Clinitalk, or that works with Clinitalk.
* Group, realises that it is a part of their role and that they have an important part to play
* Ensure the process for monitoring compliance to the information security management system (ISMS) is effective and meets Business needs
* Ensure that improvement opportunities are identified, prioritised and driven forward via the continual improvement process

This policy will be regularly communicated to all Clinitalk employees.

# Clinitalk Information Security Policy Summary:

Clinitalk will provide safe and reliable educational services for healthcare that offer our customers confidence that we manage information security risks adequately.

We will protect assets, observe legal and regulatory obligations, protect our customers, and provide business continuity. Our organization is committed to maintaining the confidentiality, integrity, and availability of information assets, including call recordings and customer data, within the context of the Clinitalk service.

This Information Security Policy establishes the framework, principles, and responsibilities for securing the online application that records consultations, in alignment with the ISO 27001 standard.

# Assessment of Internal and External Issues Impacting Business Objectives

We have determined issues impacting the business objectives both external and internal and shall review these annually.

|  |  |  |
| --- | --- | --- |
| Reviewer | Date | Comments |
| N.Boeckx | 25/9/23 | Objectives review |
|  |  |  |

|  |
| --- |
| **Issues impacting Clinitalk business objectives** |
|  | Positive | Negative |
| Internal issues | **Strengths*** Motivated staff
* Subject matter expertise (clinical and computing)
* Good relationships with key organisations (Health Education England, Royal College of GPs)
 | **Weaknesses*** New organization thus at outset lacking policies and established processes.
* New organization thus at outset lack of documentation of business risks and mitigations
* New organization thus at outset lack of internal audits on the effectiveness of security measures.
* New organization thus at outset few formal processes and rules
 |
| External issues | **Opportunities*** ISO/IEC 27001 is an opportunity to enhance confidence in the service we provide
* We have the opportunity to develop new processes that meet the business needs.
 | **Threats*** Complexity of legislation.
* Changing legislation
* Data host security
* Introducing complexity in the application may introduce risk, we will design to minimize complexity and test.
* Cybercrime
* Employees unaware of processes
* Power loss
* Inadequate backup
 |

|  |
| --- |
| **External issues for the management system** |
|  | Positive | Negative |
| External issues | **Strengths*** We have support from key external organisations (Health education England, Royal College of GPs (RCGP), University of Birmingham Research, National Institute of Healthcare Research)
* We have good access to documentation on regulatory requirements and ISO standards implementation.
* We have secured funding to support development from Innovate UK
* We have secured support for evaluation projects from Health Education England and the RCGP
* We have experience of the regulatory requirements for recording consultation audio and a template has been laid out by external organizations which we can follow.
 | **Weaknesses*** Our funding is time limited to the project period and future funding to support Clinitalk will be dependent upon success.
* Our ability to pilot is dependent upon the support of external organizations. Inadequate information security preparation could put those plans in jeopardy.
* We do not control the policies and processes in the server supplier organization and rely on external assurance of their information management standards.
 |
| **Opportunities*** Using experienced external organisations to provide server hosting and security means we benefit from their learned experience in protecting large numbers of organisations which we can build on top of through our internal processes and policies.
 | **Threats*** Business failure of our supplier would be a threat to business continuity and therefore we require an established and reliable supplier.
* Future changes in data storage regulatory requirements may require us to change our processes and policies.
 |

# Interested parties and requirements (ISO 27001 section 4.2a and b)

Our goals and objectives for information security are largely determined by our interested parties and their requirements.

 For details of our interested parties please see ‘1006 Information security management system’

# Scope (ISO 27001 section 4.3)

The goals of our information security policy are heavily influenced by its scope.

 For details of our ISMS scope please see ‘1006 Information security management system’

# Responsibilities

## The Clinitalk Board

The Clinitalk board is formed of its directors and has ultimate accountability for information security. More specifically, they protect the organisational reputation of Clinitalk by being assured that clear regulations, policies, and procedures that adhere to legislative and regulatory requirements are in place, ethical in nature, and that they are being followed.

The board needs to be assured that there are effective systems of control and risk management in effect, and that our governance structures and processes are fit for purpose, by referencing them against recognised industry standards of good practice.

The board is responsible for:

* Leading and fostering a culture that values, protects and uses information for the success of Clinitalk and for the benefit of employees, customers and other stakeholders;
* Ensuring that Clinitalk is operating within the specified Clinitalk information security risk appetite, taking into account the prevailing legal, political, socio-economic and technological environment and external standards; and
* Ensuring that a fit for purpose and adequately resourced information security programme is in place, including this policy as the top level reference document.

## Caldicott Guardian

The Clinitalk Chief Medical Officer fulfils the Caldicott Guardian role and is the senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly within the organisation.

## Senior Information Risk Officer

The Clinitalk Senior Information Risk Officer fulfils the SIRO role and is the senior person with overall responsibility for information risk and policy.

## Data Protection Officer

The Clinitalk Chief Medical Officer fulfils the DPO role and is the senior person responsible for providing direction in terms of information governance and advising the members of Clinitalk in terms of ensure that the personal data of staff, clients, customers, providers or any other individuals/ data subjects is processed in compliance to UK Data Protection laws/regulations (as well as managing interactions with the regulatory authorities).

# Policy Statements

## Governance

Clinitalk will define and implement appropriate governance arrangements for the management and accountability of information security.

## Asset Management

Critical Information Assets (including information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for.

1. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.
2. Information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and the relevant classification will indicate appropriate handling requirements.

## Access Control

1. Access to all relevant information will be controlled and access will be approved based on business needs.
2. Access will be granted, or arrangements made for users, according to their role and the classification of information to the extent necessary for the relevant individual to fulfil their role and responsibilities.
3. A formal user registration and de-registration procedure will be maintained for access to all information systems and services.
4. Mandatory authentication methods will be employed (including, where appropriate, multi-factor authentication).
5. Specific controls will be implemented for users with elevated privileges, to reduce the risk of accidental or deliberate system misuse.
6. Segregation of duties will be implemented, where practical.
7. Privileged Account Management for administrative/high-risk users will be implemented.

## Cryptography

Standards, guidance and tools will be provided to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

## Physical and Environmental Security

1. Access Control measures (including physical keys, and their management) are implemented and reviewed to ensure access to organisational buildings and further internal controlled areas is granted to authorised personnel only.
2. Critical, sensitive and otherwise protectively marked assets are stored only in secure areas with additional access controls.
3. Server Rooms are outsourced to Microsoft Azure and their security standards reviewed to ensure they are subject to security control measures (including secure, lockable entry points, CCTV control, entry/exit logs, environmental controls, uninterruptable power supplies (UPS) and locked server cabinets within).
4. Laptops and desktop devices are to be stored securely or fixed down to desks using approved locks and cables.
5. All Clinitalk locations shall undergo regular risk assessments in order to review effectiveness of controls

## IT Security

1. IT networks will be implemented with appropriate segmentation (internally, client facing and from the Internet) in effect. Measures will include continuously monitoring the network use. All users actions are logged including failed log in attempts and errors. Network access and access to systems will based on the principle of ‘least privilege’ and maintained through auditable and accountable user accounts with unique identifiers.
2. Security Incident process and procedures will be operated to respond to any critical security weaknesses which may be identified and any alerts from internal and/or external sources.
3. The production IT infrastructure will be under a programme of regular scanning for weakness.
4. IT Heath-checks and Penetration Tests will be conducted on a regular basis (based on perceived asset criticality and risks).
5. Identity and access management controls will be in place to authenticate and manage access to the network domains, applications and systems.
6. Access privileges and permissions will be regularly reviewed (and removed or limited if not required).
7. Controls against malware, including appropriate intrusion prevention/detection, will be implemented.
8. Staff are not permitted to use mobile devices for Clinitalk related work. Staff may only use devices issued by Clinitalk to access work relating to Clinitalk.
9. IT Software & Hardware Inventories will be maintained and updated.
10. Wireless and Internet controls will be implemented (encryption, authentication, access controls).
11. No software installation is required. Clniitalk runs on any modern web browser.
12. User account status shall be listed in the personnel file and reviewed and updated with administrator permissions revoked where access is no longer required.
13. All Clinitalk systems will have automatic updates enabled to ensure software is maintained and up to date. Updates will be applied to all software including operating system, database application and infrastructure. Devices will be reviewed annually to ensure that automatic updates remain enabled on all software and that systems have correctly updated.

## Cloud Security

1. Cloud based solutions utilised by Clinitalk will be reviewed with appropriate oversight and due diligence before operations commence.
2. Cloud Platform Service utilised by Clinitalk for the development and production of products/services will be subject to the National Cyber Security Centre (NCSC) Cloud Security Principles.

## Asset and Data Security

1. Information assets will be classified (according to any relevant legal requirements as well as perceived business value, criticality and sensitivity).
2. Information Asset Retention guidelines and policy will be in place.
3. Information Classification guidelines and policy will be in place.
4. Data loss prevention technical and organisation measures will be implemented to protect data in transit, at rest and across the networks/domains and in the Cloud based systems and platforms.

## Systems Acquisition, Development and Maintenance

1. Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.
2. Controls to mitigate any risks identified will be implemented where appropriate.
3. Systems development will be subject to change control and separation of test, development and operational environments.

*Change control helps in maintaining the integrity, stability, and security of systems and applications throughout their development lifecycle. Here are the key aspects of Clinitalk’s change control process:*

*Request for Change (RFC): Change control begins with the submission of a Request for Change (RFC). This can be a proposed modification, enhancement, bug fix, or any alteration to the project or system.*

*Evaluation: The proposed change is evaluated by a designated change control board or team. This evaluation considers the impact of the change on the project timeline, budget, resources, and existing functionalities.*

*Approval: Based on the evaluation, the change control board decides whether to approve or reject the proposed change. If approved, the change is documented, and necessary adjustments are made to the project plan, budget, and resources.*

*Implementation: The approved change is implemented following a predefined process. This may involve modifying the source code, updating documentation, configuring systems, or making changes to project requirements.*

*Testing: After implementation, rigorous testing is conducted to ensure that the change does not negatively impact the existing system functionality. Various types of testing, including unit testing, integration testing, and system testing, may be performed.*

*Documentation: Comprehensive documentation of the change, including the reasons for the change, the implemented modifications, and the testing results, is crucial. This documentation provides a record of the change for future reference and auditing purposes.*

*Communication: Stakeholders, team members, and relevant parties should be informed about the approved change and its implications. Clear communication ensures that everyone is aware of the modifications being made.*

*Quality Assurance: Change control processes often include quality assurance measures to guarantee that the change meets specified requirements and standards. This might involve code reviews, security assessments, or compliance checks.*

*Version Control: Changes often involve modifications to source code. Version control systems track these changes, allowing developers to collaborate effectively, revert to previous versions if necessary, and maintain code integrity.*

*Post-Implementation Review: After the change has been implemented, a post-implementation review is conducted to assess its impact on the project or system. This review helps in learning from the change process and making improvements in future change control activities.*

*By following a structured change control process, organizations can manage modifications effectively, minimize risks, maintain system stability, and ensure that changes align with project objectives and stakeholder expectations.*

## Risk Management

1. Information Security Risks will be identified, assessed, treated and recorded in line with the Clinitalk Risk Management methodology and policy.
2. The company Risk Register will be regularly updated in terms of any Security Risks.

## Third Party Risk Management

1. A Supply Chain Risk Management process will be implemented and maintained for all new and current suppliers.
2. Relevant commercial contracts with third party service providers and suppliers will, where appropriate, include Security provisions, including the right to audit.
3. The Due Diligence process will be included in the Supply Chain Risk Management process to identify security and privacy risks to determine supplier suitability.

## Information Security Incident Management

Guidance will be available on what constitutes an Information Security incident and how this should be reported.

1. Actual or suspected breaches of information security must be reported and will be investigated.
2. Appropriate corrective action will be taken and any learning built into controls.
3. An incident management policy is maintained and regularly reviewed to improve processes for all incident types and severity levels.

## Personnel Security

1. Where practical, security responsibilities will be included in role descriptions, personnel specifications and personal development plans.
2. An annual security training and awareness strategy is implemented for all staff members.
3. Appropriate personnel checks, vetting and clearances will be obtained in line with company policy.

## Business Continuity

1. Resilience arrangements will be in place to protect critical business processes from the effects of major of information systems or disasters and to ensure their timely recovery in line with documented business needs.
2. Business impact analysis will be undertaken in respect of the consequences of disasters, security failures, loss of service, and lack of service availability.
3. Business continuity plans will be maintained and tested in support of this policy.

## Compliance

* The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements.
* A combination of internal and external audits and assessments will be utilised to demonstrate compliance against selected standards and best practice, including against internal policies and procedures.

## Policy Compliance

This policy applies to all Clinitalk employees, contractors and consultants acting on behalf of Clinitalk, and they must abide by this policy.

## Non-compliance

Failure to comply with this policy could result in disciplinary action, and where a third party is involved this could result in termination of contract.

# Policy Endorsement

This policy has been agreed by:

Signed: Nicholas Boeckx, Clinitalk Chief Medical Officer

Date: 17/10/23

# Policy Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Level | Role | Responsibility |
| Policy owner | Senior Information Risk Officer (SIRO) | Develop and maintain policyReview and update policyEnsure policy is communicated and accessible |
| Policy implementation and monitoring | Group Security Team *(led by the data protection officer and senior information risk officer)* | Implement the policyEnsure process, procedures and guidelines exist to operate the policyUndertake monitoring and oversight of the policy including exceptions, non-compliance and manage escalations |
| Policy approver | Chief Operating Officer (COO) | Clinitalk Board |

# Overarching principles

## Information Classification

All information handled by the Clinitalk consultation recording software shall be classified according to its sensitivity:

 a. Highly Sensitive Information

- Personally Identifiable Information (PII) of customers.

- Sensitive financial and health data.

- Any data that can directly identify an individual.

- Call recordings and transcripts.

 b. Sensitive Information

- Customer contact information.

 c. Non-Sensitive Information

- App usage statistics and logs.

- Non-identifying call metadata.

#  4. Information Security Management System (ISMS)

 a. ISMS Establishment

- Implement and maintain an ISO 27001-compliant Information Security Management System (ISMS) based on risk assessments and business requirements.

 b. Risk Assessment

- Regularly assess and manage risks associated with information assets and the application.

- Identify, evaluate, and treat security risks in accordance with ISO 27001.

 c. Continuous Improvement

- Continuously improve the ISMS based on lessons learned and evolving threats.

 5. Access Control

 a. User Authentication

- Implement strong authentication mechanisms.

- Enforce password complexity and change policies.

- Use multi-factor authentication (MFA) for privileged access.

 b. Authorization

- Implement role-based access control (RBAC).

- Grant access based on least privilege principles.

- Regularly review and update access permissions.

 c. Session Management

- Implement session timeout mechanisms.

- Automatically log users out after a period of inactivity.

 6. Data Protection

 a. Data Encryption

- Encrypt data in transit using TLS/SSL protocols.

- Encrypt data at rest using strong encryption algorithms.

 b. Data Retention and Disposal

- Define and enforce a data retention policy.

- Securely delete or archive data when it is no longer needed.

 7. Monitoring and Logging

 a. Logging and Audit Trails

- Implement comprehensive logging mechanisms.

- Log all access and critical actions within the application.

- Retain logs for a defined period as per the retention policy.

 b. Incident Detection and Response

- Establish procedures for detecting and responding to security incidents.

- Regularly review and analyse logs for suspicious activities.

 8. Incident Response and Reporting

- Develop an incident response plan, detailing incident identification, escalation, mitigation, and recovery.

- Report security incidents promptly to relevant authorities, stakeholders, and affected parties, as required by law and regulations.

 9. Vendor and Third-Party Security

- Assess the security practices of third-party vendors and service providers.

- Ensure that third parties adhere to our security requirements and policies.

 10. Compliance with Laws and Regulations

- Maintain awareness of and comply with all applicable data protection, privacy, and information security laws and regulations.

 11. Security Awareness and Training

- Provide regular security awareness training to employees, contractors, and other relevant personnel.

- Promote a culture of security awareness within the organization.

 12. Policy Review and Compliance

- Periodically review and update this Information Security Policy to ensure alignment with ISO 27001 requirements and changing security landscapes.

- Conduct regular compliance assessments and audits.

 13. Roles and Responsibilities

- Clearly define roles and responsibilities for information security.

- Ensure accountability for the implementation and maintenance of security controls.

 14. Enforcement and Consequences

- Non-compliance with this policy may result in disciplinary actions or legal measures, as appropriate.

- Violations of this policy may result in investigations, reporting to authorities, and potential legal action.

This Information Security Policy establishes the foundation for safeguarding information assets and managing security risks within the context of our Clinitalk consultation recording software. It is the responsibility of all personnel to adhere to this policy and contribute to the ongoing protection of information and the organization.