FINANCIAL SERVICES

Company Reg No. 2006/032434/07
FSP No. 45651

PRIVACY POLICY V1.4

Version	Author	Reason for Change	Date
V1.0	i-Talk Team	Creation	11 March 2022
V1.1	i-Talk Team	Adjustment & Review	11 March 2023
V1.2	i-Talk Team	Adjustment & Review	18 March 2024
V1.3	i-Talk Team	Adjustment & Review	24 April 2024
V1.4	i-Talk Team	Adjustment & Review	22 May 2025

Last Update: 2025-05-27 04:10 PM

Index

1. Policy Statement

The risk of invading a person's privacy through the misuse of their personal data and information has been recognized in countries around the globe, many of which have established legislation to prevent the abuse and in addition to regulate the collection, processing, retention, safeguarding and use of personal data. The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy. The Protection of Personal Information Act, No.4 of 2013 ("POPIA") is aimed at facilitating the protection of this important right and comes into effect on 1 July 2021.

This Privacy Policy sets out the obligations and responsibilities of all company stakeholders who access, process, receive and/or use a data subjects' personal information in accordance with the provisions of POPIA and its underlying principles, namely the eight (8) Conditions for the Lawful Processing of Personal Information. i-Talk Financial Services respects the privacy of our employees and customer personal information which shall be protected through the use and interaction of its various business units and support functions inclusive of https://italkinternational.com/ and all associated websites, mobile applications, social media sites and/or other online services, combined with our product and service offerings where personal data is collected offline and/or received from third party providers.

In sum, this Privacy Policy describes how we at i-Talk Financial Services may collect and use personal data and information, who we share may it with, how we should protect it, along with ensuring that the different lines of our business respect the rights and choices exercised by data subjects such as customers and employees.

2. Policy Objective

The overarching aim of this internal Privacy Policy is to provide regulatory insight and operational guidance as to the controls, mechanisms and practices that need to be applied and implemented by all accountable company and group stakeholders to ensure compliance with the Protection of Personal Information Act. The primary objective of this Policy is to ensure alignment with the Privacy Notice on our website as well as the Privacy clauses contained in our agreements. Moreover, this Policy sets out to provide strategic direction to i-Talk Financial Services enabling all lines of business to timeously identify and proactively mitigate those privacy and regulatory risks that may present possible operational challenges or result in non-compliance with the Protection of Personal Information Act following its enactment. Familiarization with this Privacy Policy will assist stakeholders in conforming to the regulatory

requirements around the protection of personal information held or processed by the company at any given time.

This Policy has been created to ensure that as a responsible organization i-Talk Financial Services is in alignment with local as well as global best practice with regard to the management of regulatory risk including control and processing mechanisms around the protection of personal information and data privacy.

3. Policy Scope

This policy applies exclusively to i-Talk Financial Services and its operations within the Republic of South Africa. It encompasses our business units, subsidiaries, processes, systems, websites, as well as all directors, employees, and representatives. Compliance with this policy is essential for i-Talk Financial Services to uphold individuals' constitutional rights concerning personal information processing and to protect their right to privacy.

4. What is Personal Information?

Personal information ("PI") is defined in POPIA as information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, and includes **any information that identifies or relates specifically to you**, including, for example, your name, age and identity number or other national identifier, your contact address, your location, your banking details, e-mail and contact numbers. In short, personal information refers to any information that identifies a person or specifically relates to a person.

Some types of personal information are considered special personal information ("SPI"). These include personal information revealing or related to a person's health, racial or ethnic origin, religious or philosophical beliefs, sex life, political affiliation, or trade union membership; criminal behavior and proceedings related thereto.

5. Key Definitions

The following are some of the most applicable and essential definitions contained in POPIA:

a. "**consent**" – means any voluntary, specific, and informed expression of will in terms of which permission is given to the processing of personal information.

b. "**data subject**" – means the person to whom the personal information relates.

c. "**de-identify**" – in relation to the personal information of a data subject, means to

delete any information that:

i. identifies the data subject;

ii. can be used or manipulated by reasonably foreseeable method to identify the data subject; or

iii. can be linked by reasonably foreseeable method to other information that identifies the data subject.

d. "**electronic communication**" – means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipients terminal equipment until it is collected by the recipient.

e. "**operator**" – means a person or entity who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

f. "**processing**" – means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

i. the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;

ii. dissemination by means of transmission, distribution or making available in any other form; or

iii. merging, linking, as well as restriction, degradation, erasure or destruction of information.

g. "**regulator**" – means Information Regulator established in terms of the Act;

h. "**responsible party**" – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

i. "**unique identifier**" – means any identifier that is assigned to a data subject by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

6. Exclusions

POPIA **does not apply** to the processing of personal information:

a. for purely personal or household activities;
b. that has been de-identified;
c. processed by or on behalf of a public body for the purposes of:
    - safeguarding national security;
    - the investigation and prosecution of criminal matters;
    - processed by the cabinet and its committees or the executive council of a province; or
    - relating to the judicial functions of a court.

POPIA further provides that the Act does not apply to:

d. the processing of personal information for the purposes of journalistic, literary or artistic expression in defined circumstances;
e. the exclusion for journalistic purposes requires the journalist to be subject to a code of ethics and provides adequate safeguards for the protection of personal information.

The Regulator may grant exemptions to compliance with the Conditions for the Lawful Processing of Personal Information.

7. The Conditions for the Lawful Processing of PI

POPIA lists eight (8) conditions or principles for the lawful processing of personal information, namely:

a. **Condition 1 – Accountability**
b. **Condition 2 – Processing Limitation**
c. **Condition 3 – Purpose Specification**
d. **Condition 4 – Further Processing Limitation**
e. **Condition 5 – Information Quality**
f. **Condition 6 – Openness**
g. **Condition 7 – Security Safeguards**
h. **Condition 8 – Data Subject Participation**

8. Collection and processing of PI must be for a specified purpose

Personal information ("PI") must be **collected and processed for a specific, explicitly defined and lawful purpose** relating to a lawful function or activity of the responsible party. The **data subject must be made aware of this purpose from the outset** (for example, this provision should and would normally be included in the terms and conditions of a contract with the responsible party).

9. Lawfulness of processing PI

Personal information ("PI") must be processed lawfully and in a reasonable manner so that it does not unnecessarily infringe on the data subject's right to privacy. PI must be processed in terms of the purpose for which it was originally collected whereby:

a. the **data subject must have consented** to the processing; or
b. **processing is required for the completion of a transaction or conclusion of a contract or agreement** (for example a credit or hire-purchase agreement, a lease or buy and sell agreement, etc.) entered by the data subject; or
c. **processing is permitted in terms of a law** (for example but not limited to the Companies Act; the Consumer Protection Act (CPA); the Electronic Communications and Transaction (ECT) Act; the Financial Advisory and Intermediary Services (FAIS) Act; the Financial Intelligence Centre Act (FICA); the National Credit Act (NCA); the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) amongst other legislation); or
d. **processing permitted in terms of a public law duty of a public body** (for example but not limited to the Department of Justice (DoJ), the South African Revenue Service (SARS), the South African Police Service (SAPS), amongst others); or
e. processing protects the **legitimate interests** of the data subject; or
f. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Unless the processing of personal information is provided for in law (see criteria above), the data subject may at any time and on reasonable grounds object to the processing of his or her personal information. Consequently, the responsible party may no longer process the personal information. Furthermore, non-compliance with these provisions of POPIA may result in regulatory sanction and/or hefty penalties which could adversely impact business operations and reputation of i-Talk Financial Services.

10. Further processing limitation

In the first instance, the **further processing of personal information must be in accordance or compatible with the purpose for which it was originally collected**. Consequently, personal information collected and processed in terms of RICA for example may not be further processed for activities outside of or foreign to the permissible purposes of RICA save for any of the **exceptions listed below** that may apply.

Further processing of personal information is permissible in the following instances (i.e. exceptions) *only*:

(a) where the data subject has provided the necessary consent (must be informed and of own free will);

(b) in order to comply with an obligation imposed by a law (e.g. FICA, NCA, RICA, etc.);

(c) the personal information is available or derived from a public record or a record that has been made public by the data subject him/her-self (e.g. court judgment, telephone directory, etc.);

(d) for the detection, investigation, prevention and/or prosecution of offences (e.g. anti-money laundering activities, fraud detection and prevention, etc.);

(e) in the interests of national security;

(f) for the purposes preventing imminent or serious threat to life, health or public safety;

(g) for historical, statistical or research purposes (e.g. population census, research paper or report on consumer behavior, economic or scientific studies, etc.); or

(h) where the Information Regulator has granted permission to do so.

11. So what PI are we permitted to process at i-Talk Financial Services?

In terms of POPIA, we are required to only process personal information for lawful purposes relating to our business in any one or more of the following circumstances:

a. where an existing customer is on our customer database. This means the customer has purchased a product from us or used our services;

b. where the customer communicates, interacts and/ or transacts with us, our strategic partners, VAS providers and/ or promoters;

c. if, where required, the person has explicitly consented thereto;

d. if the person has not requested that we refrain from processing their personal information;

e. if the law or a court, has consented thereto;

f. if it is necessary to conclude or perform under a contract, we have with the person;

g. if the processing is for statistical or research purposes;

h. if the law requires or permits it; and/or

i. if it is required to protect or pursue a customers', employees' or a third party's legitimate interest.

We may process special personal information in any one or more of the following circumstances:

j. if the person has consented to the processing;

k. if the processing is needed to create, use or protect a right or obligation in law;

l. if the processing is for statistical or research purposes and all legal conditions have been met;

m. if the special personal information was made public by the person;

n. if the processing is required by law;

o. if the processing is required to identify a person; and/or

p. if health information is processed, and the processing is to determine the insurance risk of the person, or to comply with an insurance policy or to enforce an insurance right or obligation.

12. The PI we can collect

We may collect a several of types of personal information for the purposes stated in this Privacy Policy, including:

a. identifiers and contact information, such as the data subjects identity number, name, address, phone number/s, and/or email address;

b. purchase or other commercial information, such as the products and/or services the data subject may purchase and/or use, delivery address, and contact information;

c. payment information, such as payment method and payment information (such as debit or credit card number), and billing address belonging to the data subject;

d. communications and interactions, which may include e-mail messages, chat sessions, text messages, and phone calls that we and/or our strategic partners and/or service providers exchange with the customer;

e. demographic information, which may include age or birthdate, gender, postal code, the status of a customer, and other related information about the customer;

f. call recordings, including information about the customers call and what they share when they call us or we call them on the phone;

g. location or geolocation information of the customers device that they use, should their device settings allow us to collect location information;

h. device and browsing information and other Internet activity information, including information about the customers phone, tablet, computer, or device, and online browsing activity (collectively, "automatically collected information"). Automatically collected information may include IP addresses, unique device identifiers, cookie identifiers, device and browser settings and information, and Internet Service Provider (“ISP”) information. Automatically collected information also may include information about when and how the customer may access and use the distribution channels or how they interact with us on the distribution channels, such as the date and time of their visit or use, the websites they visit before coming and after leaving our distribution channels, how they navigate and what they search for using our distribution channels, the website pages and items they view using our website and other distribution channels, and the items they purchase or offers they may show an interest in; and

i. inferences about any of the information above that may relate to a customer’s preferences, or other matters; and

j. when we collect information that does not personally identify the customer, including, information that has been anonymized or aggregated, if we link this information with the customers personal information, we must treat such linked information as personal information.

Remember, the customer / data subject can choose not to provide personal information to us when requested. However, if their personal information is necessary to provide the customer with services and products and/or offers regarding the aforesaid, including access to our distribution channels, and/or to perform administrative functions, we may as a consequence be unable to perform such services.

13. How we may use PI

We may use a data subjects' personal information for the following reasons but this must always be **in line with our business and the purpose** for which the PI is collected:

a. to enable the conclusion, implementation and enforcement of transactions the data subject may enter into with us or our strategic partners for products and services;

b. to respond to the customers enquiries and/or complaints;

c. to process returns and/or refunds;

d. to provide information about products and/or services that the customer has requested and notifying them about important changes or developments to these products and/or services;

e. to follow-up as part of our customer-care process;

f. to update the data subjects' records on our customer database and other internal records;

g. to administer offers and transactions we make and/or enter into with the customer;

h. to improve our products, services and/or distribution channels;

i. to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and/or rules), voluntary and involuntary codes of conduct and industry agreements or to fulfil reporting requirements and information requests;

j. sending marketing and other communications with the latest specials, deals, alerts, notifications and promotions in relation to our business, products and

services, for marketing those products and services and to market related products, goods and services to the customer;

k. to develop, test and improve products and services for customers and making our services or those of our strategic partners and/or service providers easier for customers to use;

l. to detect, prevent and report theft, fraud, money laundering and other crimes. This may include the processing of special personal information, such as alleged criminal behavior or the supply of false, misleading or dishonest information or avoiding liability by way of deception;

m. to enforce and collect on any agreement when customers are in default or in breach of the agreement terms and conditions, for the purposes of tracing customers or to institute legal proceedings against customers;

n. to contact customers for market research purposes in relation to our business or the business of i-Talk Financial Services and to conduct market and behavioral research, including scoring and analysis to determine if customers qualify for products and services;

o. evaluating the effectiveness of our marketing and for the purpose of research, training and statistical analysis;

p. for historical, statistical and research purposes, such as market segmentation;

q. to record and/or assist appointed payment processors to process instructions payment instructions (i.e. debit order or EFT);

r. to manage and maintain customer relationships with ourselves;

s. to enable us to deliver products, services, documents or notices to customers;

t. for security, identity verification and to check the accuracy of a data subjects personal information;

u. to communicate with customers and carry out their instructions and requests;

v. for customer satisfaction surveys, promotional and other competitions;

w. to enable data subjects to take part in customer loyalty reward programmes, to determine their qualification for participation, earning of reward points, determining their rewards level, monitoring their buying behavior with our rewards partners to allocate the correct points or inform them of appropriate products, goods and services that they may be interested in or to inform our reward partners about customer purchasing behavior;

x. to enable customers to take part in and make use of VAS; and/or

y. for any other customer relationship and service-related purposes.

14. What are a data subjects rights under POPIA?

Data subjects have the right to:

a. the information we hold about their personal details.

b. access free of charge the information about themselves stored by us and its use.

c. correct, destroy, or delete this data as and where permitted in law.

d. opt-out of direct marketing calls or mail.

e. remove their data from a direct marketing list.

f. object on reasonable grounds to the processing of their personal information.

g. withdraw consent to the processing of their personal information.

The customer / data subject may formally submit a request to our Information Officer to access their personal information that the i-Talk holds on them. By using the PAIA tab / link at the bottom of the landing page of our primary website, customers / data subjects may refer to our Promotion of Access to Information Act No. 2 of 2000 Manual ("PAIA Manual") for access to their PI and further information related thereto.

Data subjects also have the right to lodge a complaint with the Information Regulator about how we process their personal information. E-mail: complaints.IR@justice.gov.za

15. What safeguards are in place to secure PI?

We must take all reasonable and appropriate technical and organizational steps to ensure that personal information is kept secure and is protected against unauthorized or unlawful processing, misuse, unauthorized disclosure, loss, interference, destruction or damage, alteration, disclosure or access.

Our security systems must be in line with industry best practice and standards. We must monitor system developments to ensure that our security protocols evolve, as required. We must test our systems regularly, viz. penetration and vulnerability testing.

Personal information must be destroyed or anonymized when no longer needed or when we are no longer required by law to retain it (whichever is the later). For further guidelines and requirements please refer to the Records Management / Records Retention Policy.

We are required to promptly notify the data subject if we become aware of any unauthorized use, disclosure, or processing of their personal information.

Where storage is in another country, personal information must be stored in a jurisdiction that has equivalent, or better, data protection legislation than South Africa or with a service provider which is subject to an agreement requiring it to observe data protection requirements equivalent to or better than those applicable in South Africa.

Notwithstanding the above, no data transmission over the Internet or data storage system can be guaranteed to be completely secure. Customers should not send us sensitive information via email. Should a customer / data subject have reason to believe that their interaction with us is not secure (for example, if they feel that the security of any account they may have with us has been compromised), they must immediately notify us of the problem by contacting us at complaints@i-talk.co.za

16. How long must we retain PI?

We may retain personal information for as long as is necessary to fulfil the purpose for which it was collected (minimum period of five (5) years) unless a longer retention period is required to comply with legal obligations, resolve disputes, protect our assets, or enforce agreements. The criteria we use to determine retention periods include whether:

a. We are under a legal, contractual or other obligation to retain personal information, or as part of an investigation or for litigation purposes;
b. Personal information is needed to maintain accurate business and financial records;
c. There are automated means to enable the customer to access and delete their personal information at any time;
d. The data subject has consented to us retaining their personal information for a longer retention period, in which case, we will retain personal information in line with their consent.

Personal information records may be retained for periods in excess than those stated above where they pertain to historical, statistical or research purposes provided i-Talk Financial Services has established the necessary safeguards against the records being used for any other purposes.

General accepted practice is to retain records for at least five (5) years after the date of the last transaction or from the date the relationship or contract was terminated, however

other legislation may call for personal and/or transactional records to be retained for longer retention periods.

Furthermore, POPIA requires a responsible party to destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorized to retain the record, i.e. after five (5) years have elapsed or where a specific law specifies a longer period. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

For further guidelines and requirements please refer to the Records Management / Records Retention Policy.

17. The sharing of PI

In general, we will only share personal information if any one or more of the following apply:

a. if the law allows it;

b. if, where necessary, the data subject has consented to this;

c. if it is necessary to conclude or perform under a contract that we or our strategic partners, promoters, VAS providers and/or clients have with the data subject / customer;

d. the data subject has specifically consented to the sharing of their personal information during an interaction or transaction through our distribution channels or other communication channel;

e. if the law requires it; and/or

f. if it is necessary to protect or pursue our interests, our or the legitimate interest of a third party.

Where permitted in law or where applicable subject to disclosure and/or informed consent, we may share personal information with the following persons. These persons have an obligation to keep the personal information secure and confidential:

g. our employees in their performance of their duties;

h. attorneys and other persons that may assist with the enforcement of agreements;

i. payment processing services providers, merchants, banks and other persons that assist with the processing of payment instructions, such as card scheme providers;

j. law enforcement and fraud prevention agencies and other persons tasked with the prevention and/or the prosecution of crime;

k. regulatory authorities, industry ombuds, governmental departments, local and international tax authorities and other persons the law requires us to share personal information with;

l. credit bureaux or other similar verification agencies;

m. our service providers, agents and sub-contractors like couriers and other persons we use to offer and provide products and services to customers;

n. persons to whom we have ceded our rights or delegated our obligations to under agreements, like where a business is sold;

o. courts of law or tribunals that require the personal information to adjudicate referrals, actions or applications;

p. the general public where customers submit content to our social media sites like our Facebook page;

q. trustees, executors or curators appointed by a court of law;

r. participating partners in our customer loyalty reward programmes, where customers purchase products and services or spend loyalty rewards;

s. our joint venture and other partners with whom we have concluded business arrangements.

18. Cookies and Similar Technologies

When customers access our Online Services or Sites ("Sites"), we may use cookies (small text files containing a unique ID number which are placed on a customers' PC or device) and similar technologies including scripts, embedded web links and web beacons. We may use cookies to assist us with activities such as:

a. Enabling customers to sign in to our Sites;

b. Authenticating customers;

c. Keeping track of information, customers have provided to us;

d. Improving customer browsing experience;

e. Customizing our interactions;

f. Storing and managing customer preferences and settings;

g. Compiling statistical data;

h. Analyzing the performance and usability of our Sites;

i. Measuring traffic patterns for our Sites; and

j. Determining which areas of our Sites have been visited.

These technologies collect information that the customer browser sends to our Sites

including browser type, information about the IP address (a unique identifier assigned to customer computer or device which allows their PC or device to communicate over the Internet), together with the date, time and duration of their visit, the pages they may view and the links they click on.

The information that we collect using cookies is non-personal information. Customers must always be free to decline our cookies if their browser permits, but some parts of our websites may not work properly should they elect to do so. We do not allow third parties to place cookies on our websites.

Our Sites may also contain web beacons or similar technologies from third party analytics providers, through which they collect information about certain customer activities across our Sites to help us compile aggregated statistics.

19. Direct Marketing

We may send customers direct marketing communications about our products and services as well as new products, promotions, special offers and other information. We will do this in person, via e-mail, SMS, WAP Push, newsletters, telephonically, or through instant chat.

Customers must be able to opt-out of receiving marketing materials from us at any time and manage their communication preferences by:

a. Following the unsubscribe instructions included in each marketing communication from us or telling us they wish to unsubscribe;
b. Sending an email to the sender of the marketing communications; or
c. Registering on the Do Not Contact list of the Direct Marketing Association of South Africa which can be found on www.dmasa.org
d. Including their details and a description of the marketing material they no longer wish to receive from us.
e. We must comply with such customer requests as soon as is reasonably practicable but no longer than 30 days.

Should a customer elect to opt-out of receiving marketing related communications from us, we may still send them administrative or operational messages as part of their ongoing use of our products and services which they will be unable to opt-out of.

We may not provide customer personal information to unaffiliated third parties for direct marketing purposes or sell, rent, distribute or otherwise make personal information commercially available to unaffiliated third parties, whatsoever.

In all cases, the customer may request us to stop sending marketing communications to them at any time.

20. Network Security

iTalk has implemented various network security measures to protect the data and resources from unauthorized access. The following are the main features of network security:

- Firewalls: installed firewalls across the network to filter the incoming and outgoing traffic based on predefined rules. Firewalls also provide user access control to servers and wireless devices.

- VLANs: iTalk has segmented the network into different virtual LANs (VLANs) to isolate the devices and data based on their functions and security levels. VLANs help to reduce network congestion and improve performance and security.

- IPSEC tunnels: The user has established IPSEC tunnels between the site and the cloud environment to encrypt and authenticate the data in transit. IPSEC tunnels provide secure and reliable communication over the internet.

iTalk has followed the best network security practices to ensure the confidentiality, integrity, and availability of data and resources.

Wireless networks: iTalk has also set up different wireless networks for various purposes and users. For example, there is a wireless network for staff, a wireless network for guests, and a wireless network for IoT devices. Each wireless network has different rules and policies to control what can be browsed and accessed online. This way, iTalk can prevent unauthorized access, protect sensitive data, and limit bandwidth usage. Wireless networks are secured with strong encryption and authentication methods.

21. ITalk2u (System)

Encrypted Data Transmission

iTALK2U employs state-of-the-art encryption protocols to safeguard the confidentiality and integrity of all data transmitted within the application.

- **Transport Layer Security (TLS)**: All communications between clients and the iTALK2U server are encrypted using TLS, ensuring that data remains secure during transit over the internet. TLS employs strong cryptographic algorithms to prevent unauthorized access or interception of sensitive information.

- **End-to-End Encryption**: In addition to TLS, iTALK2U implements end-to-end encryption for voice calls, chat messages, and other forms of communication. This means that data is encrypted on the client-side before transmission and can only be decrypted by the intended recipient, providing an extra layer of protection against eavesdropping and unauthorized access.

- **Data Encryption at Rest**: iTALK2U also encrypts data stored on its servers, ensuring that even if physical access is compromised, the data remains unreadable without the appropriate decryption keys.

Role-Based Access Control (RBAC)

iTALK2U employs role-based access control to restrict access to sensitive features and data within the application.

- **Roles**: Different roles are defined within iTALK2U, each with specific permissions and access levels based on the user's responsibilities and requirements. For example, administrators have full access to all features and settings, while agents only have access to customer information relevant to their assigned tasks.

- **Permissions**: Permissions are assigned to each role, governing what actions users can perform within the application. These permissions can be finely tuned to ensure that users have access only to the functionalities necessary for their job roles, reducing the risk of unauthorized access or misuse of data.

- **Access Control Lists (ACLs)**: iTALK2U utilizes access control lists to enforce

RBAC policies, specifying which roles are allowed to access certain resources or perform specific actions. This granular control ensures that users can only access the data and features required to fulfil their duties, enhancing overall security and privacy.

Compliance Auditing

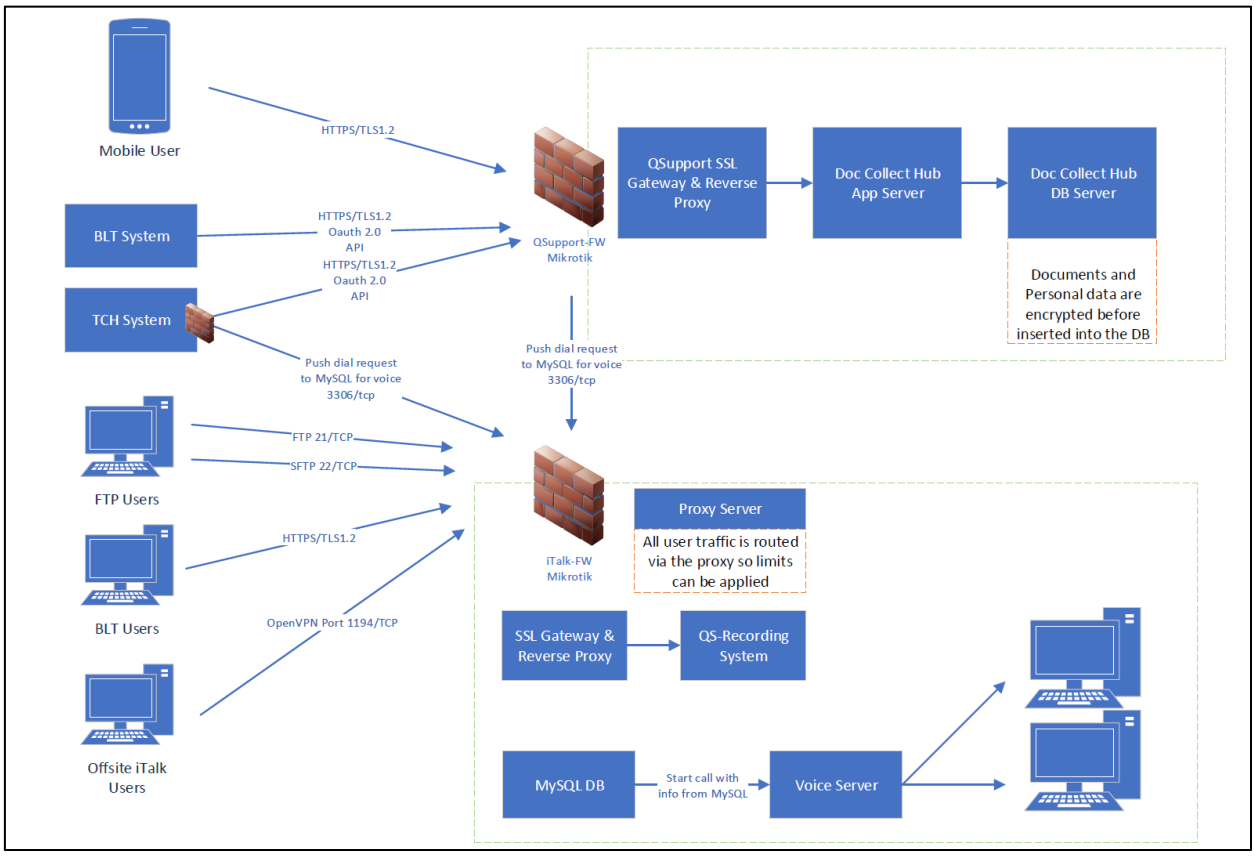
iTALK2U provides comprehensive compliance auditing capabilities, allowing clients to monitor and track changes to their data privacy controls and ensure regulatory compliance.

- **Audit Logs**: iTALK2U maintains detailed audit logs that record all user activities, system events, and configuration changes within the application. These logs capture information such as user logins, data access attempts, and modifications to access control settings.

- **Compliance Reports**: Clients can generate compliance reports within iTALK2U, summarizing the results of audits and highlighting any non-compliance issues or security vulnerabilities. These reports can be customized to meet the specific requirements of regulatory frameworks such as POPI, HIPAA, or PCI DSS.

- **Automated Compliance Checks**: iTALK2U offers automated compliance checks that regularly assess the application's adherence to data privacy regulations and industry standards. Clients can configure these checks to run at predefined intervals and receive alerts or notifications regarding any compliance deviations or potential security risks.

Compliance Infrastructure for Client



22. QS Recordings – A Web-Based Recordings Management System

A brief overview of the system's functionality and security.

What is QS Recordings?

- QS Recordings is a web-based system that allows users to access, manage, and download recordings.
- The system is designed to provide a secure and convenient way of storing and retrieving recordings without installing software or hardware.
- The system is compatible with most web browsers and can handle different audio file formats.

How do QS Recordings work?

- To use QS Recordings, users must register and log in with their credentials.
- Users can then play, listen, and download depending on their user rights and permissions.
- Users can also search for recordings by keywords, date, duration, or category.
- Users cannot share files with other users without prior access being granted.

Security Protocols.

- QS Recordings offers several advantages for users who need to access and manage recordings, such as:
- Security: The system uses encryption and authentication to protect the files, and any activity on the system is logged and traceable.
- QS recordings is only accessible via LAN or VPN, ensuring no unauthorized parties can access it outside the iTalk network.
- Convenience: The system is accessible from any web browser and device and does not require installation or maintenance. Users can upload and download recordings with a few clicks and access them anytime and anywhere.
- Efficiency: The system handles large volumes of recordings and processes and streams them quickly and smoothly.

23. Document Collection

- Doc Collect Hub is a Web Application
- Access to this application is controlled via user access levels which is used to allow limited access to defined users as per i-Talk's requirements.
- User access is controlled via username/password as well as One Time pins via SMS or email.
- Client interaction with the application will require them to login using their own ID number to prevent info sent to an incorrect person being able to submit documents, no personal information is displayed on the client interface.
- All data stored in the Data base is encrypted using AES-256 encryption and is hosted in South Africa
- Documents received from client's are scanned for malicious software and then converted to PDF.

24. Transfer of PI across the borders of South Africa

A Responsible Party in the Republic may not transfer personal information about a data subject to a third party which is in a foreign country unless adequate levels of protection are provided by:

a. the laws of that country;

b. binding corporate rules of the Operator to which information is provided;

c. a binding agreement between the Responsible Party in the Republic and the Operator in the foreign country;

d. the law, corporate rules or binding agreement must effectively uphold the principles of reasonable processing, similar to the Conditions of Lawful Processing in Chapter 3 of POPIA.

25. I-Talk Information Officer

In terms of the Promotion of Access to Information Act (PAIA) and now POPIA, i-Talk (or the responsible party) must appoint and register a designated Information Officer to ensure compliance to the Act and to liaise with the office of Information Regulator. All complaints, enquiries, and investigations with regard to personal information and data privacy (as outlined in the policy above) must be referred to the i-Talk Information Officer.

If you have any questions about how personal data should be handled by i-Talk, you have

a privacy concern or you wish to escalate a request or a complaint relating to personal information, please contact our Data Privacy Office at the following email address: compliance@i-talk.co.za

26. Data Privacy Champions

In order not to fall short of our privacy obligations and to assist with the inherent privacy challenges across the organization, Data Privacy Champions will be strategically appointed to assist with promoting the POPIA compliance programme within their own teams and to help build a privacy culture to support the business with its compliance objectives.

27. Training and Awareness

Training and awareness are among the most important risk areas when it comes to data privacy readiness and ensuring POPIA compliance within i-Talk Financial Services. To ensure accountability for data privacy across the organization, data privacy training and awareness will take place at every level of the organization.

Consequently, all employees and management within the business must be trained and made aware of the provisions of POPIA on an ongoing basis. These initiatives will foster the adoption of a privacy by design approach whereby training and awareness are the backbone of the organization's data privacy culture and its compliance journey as a whole.

28. Related and Applicable Policies

This policy must be read in conjunction with the following policies:

a. The Promotion of Access to Information Act (PAIA) Manual and Policy
b. The Data Breach and Notification Policy
c. The Data Subject Access Request Policy
d. The Records Management Policy / The Records Retention Policy
e. The i-Talk website Privacy Notice.