1: Ethical Business Plan

1.A Company Name

iSpeach

1.B.1 Goals

Our goal, Getting funded and being recognized by one or multiple qualified and well-known institutions. As mentioned in one of our OKRs, Reaching this goal means structure, confidence, and future. We believe that this generation is quite busy, expensive, and everyone feels different talking or socialising with people while having issues. This is why we connect AI with healthcare. This will help people practice without being judged during that period. We plan on connecting healthcare, rehabilitation facilities, and educational facilities to people by using their daily use mobile or any personal devices with minimal requirements.

1.B.2 Idea Origination

Most of the world communicates using English verbally and also in written form. Some people are more insecure about how they sound while they try to communicate with others, it may be because of their accents or speech disability. We aim to help people and the younger generation speak and communicate in a way that brings them confidence without being judged by someone - who might hear you or help you practice.

1.B.3 Purpose/Values/Mission

Aversive Racism, leads people to stereotyping a certain group of people whether it be because of how they look, act, sound, or their cultural/personal practices. This company aims to decrease that stereotype in the parts where people get insecure or lead them to feeling targeted by stereotyping or Aversive racism by the way they sound. We may not be able to stop Aversive Racism or stereotyping in this area but we aim to do our best to reduce it. We value privacy the most and the customer is always right.

1.B.4 Key Questions

- *How do we plan on verifying our data while keeping privacy and using AI?*

➢ *We plan on using an open source system where everyone's input and output is anonymous or only selected by the user. To verify our data using open source data, qualified and licensed personnel will verify those anonymous outputs and inputs and help create a more purified data that can be used. The use for AI, its job is simply, to only test the user on multiple data and gather data while giving constructive feedback to the user on how they may improve.*

- *Who are we to judge what is the "right" way to sound or communicate?*
- ➢ *We don't select how people should speak and communicate. The user will have all the options to select from various options on what they believe they sound like and how they want to. But in case a medical or rehabilitation facility uses our data, the doctor or the qualified personnel will have the option to select for the user and track their progress IF the user wants to or agrees to.*

1.C.1.1 OKR 1 Objective and Key Result

By March 15, 2026(Q1), iSpeech will run a production fail drill, where active clinics and in-home clients will be targeted. Client sessions will remain usiable in ≥ 99% check-ins

Objective: Reliability & Uptime (Q1 2026)
Key Results

1. Server uptime ≥ 99.9% monthly uptime
2. When the system is under load, 95% of requests wait less than 2 seconds in the queue,
3. It takes ≤ 5 minutes to detect maintenance problem (automated/user)

Customer-involving milestone/checkpoint: production drill

Stakeholders:

- **End-users:** Outages in iSpeech block the end-users' right to speech and uptime for iSpeechis critical.

- **Healthcare:** agencies and clinics are affected during client sessions and drill validations and are vested when therapy sessions, evaluations, or documentation are in place.

- **Business:** categories such as school districts, insurers, and employers are affected through renewal/payment cycles and convergence decisions.

- **Technical:** interest consists of in-house engineering, support, cloud, and vendors, where fulfillment and production are responsibilities.

- **regulatory** compliance is aimed toward government, where held offices ensure iSpeech is in compliance with regulatory requirements.

1.C.1.2 OKR 1 Metric(s) with Experiment(s)

Server uptime ≥ 99.9% monthly uptime:

In this experiment, we will measure the recorded monthly uptime against the target mentioned in KR. The 99.9% monthly uptime equates to approximately 43 minutes during a given period of 30 days, we will use this value in our experiment design.

The experiment will be validated in either a pass-or-fail rubric, where if recorded availability is ≥ 99.9%, we pass; otherwise, fail.

Population for the experiment will consist of ≥ 10 clinics and ≥ 300 in-home end-users.

iSpeech will check the session API every 30 seconds from multiple sample locations. Downtime will count if the population fails to connect. We will take the recorded and compare it to our error budget of 43 minutes.

When the system is under load, 95% of requests wait less than 2 seconds in the queue

n this experiment, we determine if ≥ 95% of the requests are ≤ 2.0s across our population.

The experiment will be validated in either a pass-or-fail rubric, where if recorded wait time ≥ 2.0s for ≥ 95% of requests, the experiment will result in a pass; otherwise, fail.

The population for the experiment will consist of ≥ 10 clinics and ≥ 300 in-home end-users.

iSpeech will track when each request enters and leaves the queue across the population. The results will be reviewed during periods of load. Results will be measured against the error budget of up to 5% of requests that may exceed 2.0 seconds. Results will be validated as Pass or Fail.

It takes ≤ 5 minutes to detect maintenance problem (automated/user):
In this experiment, we will measure the time from incident of first alert to detection from iSpeech.

The experiment will be validated in either a pass-or-fail rubric, where if 95% of incidents have detection time ≤ 5:00, the experiment will pass; otherwise, fail.

The population for the experiment will consist of ≥ 10 clinics and ≥ 300 in-home end-users.

iSpeech will check the endpoints every 30 seconds from the population. This will require two consecutive failures to start the clock. We will compare our average detection to the error budget and validate pass or fail. The error budget is up to 5% of incidents that may exceed 5:00

1.C.1.3 OKR 1 Ethical Impact(s)/Issues(s)

Potential Ethical Issues: One major ethical risk present in both Louis et al. v. SafeRent Solutions (2022) and our fictitious start-up iSpeechis the potential for bias in our dataset. It was said, “The data used … models are not neutral; it’s a mirror of inequalities from the past. It has striking effects on people’s life chances.”[1] It is impossible to create a dataset perfectly representative of demographics and contemporary standards. The model in both Louis et al. v. SafeRent Solutions (2022) and iSpeech may inadvertently reproduce past bias.

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights
End-User	Mid	High	High	High
Healthcare	Mid	High	Mid	High
Business	High	Mid	High	Mid
Technical	Mid	Mid	Mid	Mid
Regulatory	Low	Low	Low	Low

Analysis of Risks:

- **End-User:** The end-user faces mid financial risk exposure; privacy risk is high because of data/info leaks; conflict of interest risk is high; end-users face violations of right with high tolerance.
- **Healthcare:** Financial risk is mid with liability exposure; privacy risk is high; conflicting interest is high with clinics prioritize speed over in-patients' rights; violation of rights is high.
- **Business:** Financial risk is high; privacy risk is mid; conflicting interest is high considering budgetary pressure in pursuit of usability; violation of rights is low with gaps in accommodation.
- **Technical:** financial risk is mid; privacy risk is mid with engineers and in-house development that may require user data; Conflict of interest is mid with managing speed of production that may conflict with providing best and most accurate product; violation of rights is mid.
- **Regulatory:** Financial risk is low with audits and oversight; Privacy risk is low because regulators do not handle raw data; Conflict of interest is low because the rules and laws are enforced; Violation of rights is low since harms don’t affect the end-user.

1.C.1.4 OKR 1 Ethical Safeguards

1. **Test with Real Accents:** Both engineers and volunteers would help to design this safeguard. This would be implemented through adding common phrases and having a panel of diverse demographics analyze them. If there are gaps in any group, don't ship the model. this would be measured through a proprietary Gap score that tracks differences across groups. A similar process was described in Software Fairness Testing in Practice, "We had to introduce people of different skin tones and watched how the algorithm responded to each of them."[2], this safeguard results in the inclusion and across demographics. T
2. **Auto-Delete:** Engineers would help in the design of this safeguard. Through collection of logs, we would auto purge by default. Additionally, we would offer a delete my data option to end-users. This would be measured through percent of requests and time between purge.
3. **Essential Phrases:** A recurrent drill where engineers and testers design the safeguard. There would be a set of phrases that iSpeech would switch to when offline mode is activated. We would validate through tests of a fake outage. To measure, we would look at the rate of tickets from downtime from end-users.

1.C.2.1 OKR 2 Objective and Key Result

iSpeech is aiming to connect AI and healthcare in a way that the consumer can tailor their artificial assistant the way they want. One of our OKR is to get investors or a hospital/medical facility collab

Objective: Getting either funding from investors or a partnership/collaboration with a medical facility or medical educational institution by 2026(Q1),.
Key Results: Access to more opportunities to get more data and aid .
Customer-involving milestone/checkpoint: 30-day pilot / usability study of iSpeech with real customers.
Steakholders

- **Customers:** individuals using the software for speech and vocal assist.
- **Healthcare Providers:** professionals reviewing data from open source and other sources.
- **Company Engineers:** responsible for improving data accuracy and app building like AI agent .
- **Regulatory Bodies:** overseeing compliance with data security and medical privacy l

1.C.2.2 OKR 2 Metric(s) with Experiment(s)

Getting to either of those objectives would allow us to get doctor-verified and better data. To be specific, we do not have any relatable measurements or any other data as of right now because there is no similar company or business like this one.

Metrics to Measure Success:

1. **User Accuracy Rating:** On a scale of 1–10, how accurately users feel the system detects speech impairment or trouble and how well is it fixing/handling it.
2. **User Retention Rate:** Percentage of users using the software for 6+ months and by how much is it improving the user's vocal and speech skills using our platform.
3. **Healthcare Validation:** Doctor-verified accuracy and verification of open source data.

Experimentation Plan:
To evaluate accuracy, a usability study will include 50-500 participants from different demographics with speech disabilities or issues. Each participant will use the app for 30 days while logging self-reported improvements or not and issues as well. The medical personnel will be checking for accuracy.
Surveys will collect comprehensive data using Likert scales and open-ended questions. Quantitative results will determine whether the product meets its 90% satisfaction OKR. The Data will track active users and generate real-time metrics to help personnel improve our software and our AI agent.

iSpeech's main concern would be regarding data safety and privacy risk. As we will be using voices and recording them for AI agent development and for data, a data breach might be really dangerous.

As per real life cases, we've seen that consumers may connect it to aversive racism in some cases considering everyone has different speech accents.

Real-World Case Reference:
The SafeRent VS louis et al case is a clear demonstration of an aversive racism case by a software. Here Plaintiff accused SafeRent for giving increased rent and insurance just because their demographic was a certain. Similar issues may arise with the company.

1.C.2.3 OKR 2 Ethical Impact(s)/Issues(s)

- **Privacy Risks:** Unauthorized data access or breaches could expose users information like voice recordings and such.
- **Bias in Data Interpretation:** If training data lacks diversity, AI agent bias may result in inaccurate accent detection for certain demographics.

- **Conflicting Interests:** The company may prioritize commercial data analytics over individual privacy.

Expected Ethical Impact Risk Table:

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk
Customer	Low	High	Mid
Company	High	High	Mid
Investor/Medical institute	High	Low	Mid

Analysis of Risks:

- **Customers** face high privacy risks if neural data is not properly anonymized.
- **The Company** faces financial and reputation risks if ethical safeguards fail.
- **Healthcare Providers** risk professional relationships and credibility if inaccurate or biased data informs regularly.

Data transparency and leaks, So to overcome that we will be using anonymous bug reporting and also the option to select whether they want to identify and send their details to better help debug problems.

Aversive Racism, To solve that we will be giving customers multiple options to select their accents that they want to learn in and their current accent based on their opinion.

The entire control and outcome will be in the hands of the customer. In some cases the healthcare institute, if they do collaborate or use the software, will be at risk for their selection of preference for the customer. Hence it will not make the company at risk of any kind.

1.C.2.4 OKR 2 Ethical Safeguards

1. **Data Transparency Alerts:** A clear visual indicator and a screen on the app when data collection is active, with an option to see which data was shared. Designed with input from UI/UX and ethics experts.
2. **Anonymized Cloud Storage:** All personal identifiers removed before cloud transfer, ensuring compliance with GDPR and HIPAA standards.
3. **Bias Testing Protocol:** Regular independent audits by AI ethics researchers to verify that algorithms are unbiased across demographic groups.

Safeguards will be co-designed with medical ethics advisors and verified by external auditors. Effectiveness will be measured through periodic privacy compliance reviews, user trust surveys, and bias detection metrics. All the Computing ethics will be complied with the ACM code of ethics and reviewed by external auditors.

1.C.3.1 OKR 3 Objective and Key Result

Objective: Implement data privacy consent framework for recordings.
Key Results:

1. implement mandatory concent form affecting 100% of platform users.
2. implement data deletion request where ≥ 95% of request are processes in ≤ 14 days .

Customer-involving milestone/checkpoint:
Steakholders:

- **End-users:** voice recording are sensitive data and end-users should have control over how their speech is used.
- **Healthcare:** Clinics and adjecent agencies need assurances that data is documented and captured with concent.
- **Business:** Strong documentation and consent allows for assurance in liability concerns.
- **Technical:** Enginnering and in-house staff must abide by consent status and deletion request.
- **regulatory:** Govemernent bodies assure privacy rights and regulatorey enformenct over iSpeach.

1.C.3.2 OKR 3 Metric(s) with Experiment(s)

implement mandatory concent form affecting 100% of platform users:

In this experiment, we will measure the recorded consent completion rate against the target mentioned in the KR. The 100% completion target equates to all active platform users having a signed consent form on file within the measurement window; we will use this value in our experiment design.

The experiment will be validated in either a pass-or-fail rubric, where if recorded consent completion is 100% of active users, we pass; otherwise, fail.

Population for the experiment will consist of all active platform users across ≥ 10 clinics and ≥ 300 in-home end-users.

iSpeach will check for consent status at login or at first use of recording features.
Non-compliance will count if the population can access recording features without a stored consent form. We will take the recorded completion rate and compare it to our target of 100% coverage.

implement data deletion request where ≥ 95% of request are processes in ≤ 14 days .

In this experiment, we will measure the recorded completion time for data deletion requests against the target mentioned in the KR. The ≥ 95% processed within ≤ 14 days target equates to at least 95% of valid deletion requests being fully completed within a 14-day window; we will use this value in our experiment design.

The experiment will be validated in either a pass-or-fail rubric, where if ≥ 95% of valid data deletion requests are completed within 14 days, we pass; otherwise, fail.

Population for the experiment will consist of all valid data deletion requests submitted by platform users during the measurement period, including users across ≥ 10 clinics and ≥ 300 in-home end-users.

iSpeech will log each deletion request with a timestamp at submission and a timestamp at completion. Non-compliance will count if a request remains incomplete or exceeds the 14-day window. We will take the recorded completion rate and compare it to our target of ≥ 95% of requests processed within 14 days.

1.C.3.3 OKR 3 Ethical Impact(s)/Issues(s)

- **Coercion:** End-users may be under a state of duress when signing up for iSpeech. This state may pressure them into signing what anything that gives them the ability to speech.
- **Uninformed consent:** Simple app-based consent agreements may risk uninformed consent for the end-user. These end-users may accept to an agreement they don't understand or have not read.
- **Vulnerable populations**: Many end-users may have incapacity to agree to contract. These populations could include children or those with mental impotence

Stakeholder	Financial Risk	Privacy Risk	Conflicting	Violation of

			Interest Risk	Rights
End-User	Low	High	Mid	High
Healthcare	Mid	High	Mid	High
Business	High	High	High	Mid
Technical	Low	Mid	Mid	Low
Regulatory	Low	Low	Low	Low

Analysis of Risks:

- **End-users:** End-users are subject to high risk in both violation of rights and privacy risk, this can be due to the fact that voice recording are personal information. While privacy and conflicting interest risk are lower, these are still important.
- **Healthcare:** Healthcare clinics may face fines if privacy is mishandled, leading to the mid financial risk. Privacy risk is high for this group considering healthcare professionals process and handle sensitive information to the patient. Conflicting interest is low, likely due to the legal frameworks about privacy and data collection. Violation of rights is high due to the patients' rights, wherein consent for data must be obliged.
- **Business:** These bodies face high financial risk due to liability and legal reasons. Privacy risk and conflicting interest risk are also high, we can see this is due to the aggregate of data and misaligned incentive for business patient relationship. Violation rights is labeled mid, violation of rights comes down to privacy concerns and the ability for the business to follow rules.
- **Technical:** In technical stakeholders, we see low financial risk and violation of rights. Violation of rights is low when considering that technical staff implements policies the define privacy rights and financial risk does to directly bear upon staff. These technical staff is not subject to lower revenue or fines in the same way of legal entities. Privacy risk and conflicting of interest risk are seen as mid since technical staff creates the product and deals with user information and automation.
- **regulatory:**Regulatory bodies face low risk in financial, privacy risk, conflicting interest risk, and violation of rights risk. These regulatory bodies don't deal with the personal data in the same way as the other stakeholders. These regulatory bodies are primarily concerned with enforcing law and individual rights.

1.C.3.4 OKR 3 Ethical Safeguard

Anti-Coercion Safeguard: To reduce coercion, iSpeech will implement access to essential speech functionality without requiring any consent. These functionality will be designated “emergency” and or “limited” and where minimal to no data will be collected from the end-user.

With these measures in place, we can assure that core functionality is available to everyone and that no one is forced to consent to access product.
Vulnerable Populations Safeguard: Vulnerable Populations Safeguard: Many user may not have the capacity to consent, we will address this in the signup process. During signup, a parent or legal guardian will have the ability to consent for the user. This will be alongside implementations that detect if user need this functionality.
In-Time Notices: In-Time Notices: iSpeech will implement In-Time notices to user whom opt in for supplemental signup. The In-Time notices serve to offer content forms whenever a privacy risk feature is selected. There will prompt offering TOS and option to “allow” or “not now”.

1: Cultural Policy

2.A. Core Values

Our foundation is all about creating a place where everyone aims to help people feel less insecure and more confident on how they show themselves.

Transparency, we want to be known for being open and honest about how our tools work, how data is used, and how we protect our community. Because we operate in a space connected to personal presentation and self-image, we understand that privacy and clarity are essential. We view transparency as a form of respect; users deserve to understand the systems that support them.

Culture, we aim to serve people of all backgrounds, identities, and levels of confidence. We want to create products that celebrate diversity and challenge harmful stereotypes or such.

2.B. Motivation

What we love is the idea of helping people discover the version of themselves they feel proud of. We love creativity, self-expression, and the transformative effect that confidence can have on someone’s life. We are motivated by the stories of individuals who want to present themselves authentically but feel held back by fear or insecurity. The possibility of creating technology that makes people feel braver and more comfortable in their own skin inspires us every day. We also love innovation—finding new ways to blend emotional insight, ethical design, and modern tech to improve the human experience.

What we fear is contributing to the cycle of comparison, pressure, or unrealistic expectations that so many people already struggle with. We fear becoming a company that unintentionally harms the very people we want to support. We also fear losing sight of our mission by prioritizing performance metrics over well-being. Because we operate in a tech landscape where algorithms often amplify insecurity, we are aware of the responsibility we carry. Our fear drives us to build carefully, question ourselves, and implement strong ethical guardrails that keep user well-being at the center of every decision.

2.C. Summary

Confidence, authenticity, empathy, inclusion, trust, empowerment.

---

3 : Ethics Policy

3.A Core Items

Privacy: At iSpeach, privacy means user voice recordings and data will be treated in accordance with the end-user's will. End-users should know what data is being collected about them and subsequently have a say whether, if, and how that data is being used. In addition, it is our responsibility at iSpeach to protect this data and limit use and misuse. Responsibilities include storing and encrypting data, retroactively deleting data, preventing unauthorized data access or breaches, and safeguard strategies such as Auto-Delete.

Conscent We define consent through the end-user being both voluntary and informed. Respecting individuals' digital autonomy is in alignment with our core values at iSpeach. Providing clear language and ensuring that those who agree to our TOS understand where and how their data is being used. It is our responsibility that our users are aware of what they agree to, and we have implemented measures to ensure this through safeguard strategies such as Anti-Coercion, Vulnerable Populations, and In-Time Notices.

Reliability & Autonomy: Both reliability and autonomy are important to our mission at iSpeach. Through reliability, we give the user autonomy with their voice. Reliability to us not only means consistent server uptime and quick support for queries but also reliable services in the quality of speech. We achieve this through safeguard measures such as Tests with Real Accents, Essential Phrases, and Bias in Data Interpretation.

3.B. Board

Frances Haugen: An American data scientist and product manager. With degrees in electrical and computer engineering from Olin College and an MBA from Harvard. He worked in the industry from 2006–2021, working for companies such as Google, Yelp, Pinterest, Hinge, and Meta. It wasn't until 2020, where his name was pushed into the spotlight for whistleblowing on his former employer Meta. In these subsequent years he published the "Facebook Files." Frances demonstrated not only technical expertise in the tech industry but moral integrity. Where Meta prioritized profits over public safety and user security. iSpeech affirmation core items, particularly privacy and consent, align with what Frances demonstrated in his time at Meta.

Jayshree Ullal: Moved to the United States where she pursued higher education in engineering management and leadership at San Francisco State University and Santa Clara University. For 30 years she worked in the technology industry, with longstead roles at AMD, Cisco, and Arista Networks where she is currently president and CEO. Much of Jayshree career was that of overseeing data centers and managing systems, and her expertise tightly aligns with our core items of reliability. Additionally, her role in leadership and education in engineering management and roles of VP and CEO for former companies lend to her ability to lead and manage.

Tristan Harris: From Stanford University with a degree in computer science. Proceeding his education at Stanford, he studied at the Persuasive Technology Lab where he explored how to design technology to change human behaviour. Later going on to co-found Apture, a search engine optimization. His company later went on to be acquired by Google, where he found the role of product manager. Where at Google he found himself dissatisfied with practice, going to present an infamous presentation titled "A Call to Minimize Distraction & Respect Users' Attention." Tristan would later go on to be appointed the role Design Ethicist at Google. With aforementioned roles such as Design Ethicist to attest for his interest in ethical implication of computer design, his expertise and research attest to how digital products intertwine cognitive process, prove him to a perfect candidate for the board at iSpeach.

References

1. Complaint, Louis v. SafeRent Solutions, LLC and Metropolitan Management Group, LLC, Case No. 1:22-cv-10800, U.S. District Court for the District of Massachusetts, filed May 25, 2022.
2. R. de Souza Santos, M. de Morais Leça, R. Santos, and C. Magalhães. 2025. Software Fairness Testing in Practice. arXiv preprint arXiv:2506.17095. https://arxiv.org/abs/2506.17095
3. Association for Computing Machinery. 2018. *ACM Code of Ethics and Professional Conduct.* ACM. Retrieved October 12, 2025 from https://www.acm.org/code-of-ethics
4. Louis, D., et al. v. Saferent Solutions, LLC, No. 1:23-cv-01168 (D.D.C. 2023).
5.