1: Ethical Business Plan

1.A. *Company Name:* Sentinel Sphere Incorporated

1.B. *Long-Term Vision Statement:* At Sentinel Sphere Inc., we believe smart home technology should prioritize privacy, security, and user control. Our goal is to develop privacy-oriented smart home solutions using advanced edge computing, encryption, and AI-driven automation. With SafeHaven, we hope to give users full control over their data while ensuring a seamless and secure home automation experience. Looking forward, we want to set a new industry standard for ethical AI and data encryption, ensuring that privacy remains at the core of smart home innovation.

1.B.1 *Goals:* Sentinel Sphere Inc. aims to redefine smart home technology by creating a privacy-oriented AI assistant, SafeHaven, that prioritizes user control over personal data. Our primary goals include: (I) Developing a secure, intelligent, and efficient smart home assistant that operates primarily through edge computing (local data storage and management). (II) Ensuring data privacy and security by implementing end-to-end encryption and local voice processing, minimizing reliance on cloud-based storage. (III) Enhancing home automation efficiency while reducing energy consumption, by working with energy companies. (IIII) Enhance energy efficiency by integrating AI-driven sustainability features that reduce household energy consumption by at least 15%. (V) Expand accessibility and affordability by developing cost-effective versions of SafeHaven for broader consumer adoption.

1.B.2 Idea Origination: The idea for SafeHaven originated from recognizing critical privacy and security flaws in existing smart home technology. Many smart assistants rely heavily on cloud computing, increasing the risk of data breaches and unauthorized access. This concern became evident through academic discussions on AI ethics, real-world cybersecurity challenges,

and growing consumer demand for privacy-focused alternatives. By utilizing local data processing and encrypted storage, SafeHaven was designed as a trustworthy, efficient, and privacy-first solution for modern smart homes.

1.B.3 *Purpose/Values/Mission:*

Sentinel Sphere Inc. exists to empower homeowners and renters to take full control over their personal data while benefiting from an intelligent, secure, and efficient home environment. SafeHave, our main product, was designed with the core focus of privacy and user autonomy. By leveraging edge computing and local processing, SafeHaven ensures that sensitive information is stored securely on the user's device, rather than being transmitted to external servers. This approach gives users peace of mind, knowing that their data is protected from unauthorized access. The company's core values emphasized privacy first, transparency in data usage, innovation with responsibility, user empowerment, and sustainability. We believe that every individual deserves control over their personal data and should be fully informed about how it is used. Our mission is to lead the smart home technology industry by delivering an AI-powered, privacy-first home assistant that fosters trust and allows users to create a secure, personalized living space while contributing to sustainability through efficient energy consumption.

1.B.4 *Key Questions*

In order to guide the company into achieving its goals, one of the questions we must ask ourselves is: How can we consistently innovate to maintain and enhance user privacy and security while delivering smart home functionality? Another question we will ask ourselves is: How can we effectively balance accessibility and affordability with a high quality, privacy focused technology such as SafeHaven that affects a broad and diverse user base? These are

guiding questions that will be answered through our proposed objectives and key results that will help us achieve our goal.

1.C.1.1 OKR 1 Objective and Key Result

Sentinel Sphere Inc. aims to enhance user privacy by ensuring all interactions with SafeHaven remain secure through the implementation of end-to-end encryption and local voice processing, reducing the reliance on cloud storage by 75%. This milestone will be achieved by utilizing advanced encryption methods, local AI processing, and a transparent data access dashboard that allows users to manage their data. By prioritizing privacy, SafeHaven will provide homeowners and renters with a secure and efficient smart home experience that minimizes the risk of data breaches.

To reach this goal, Sentinel Sphere Inc. will work with security experts, AI developers, software engineers, and device manufacturers to optimize SafeHaven's privacy features without compromising performance. Energy companies will also play a role by integrating SafeHaven's smart energy efficiency solutions while following strict privacy standards. In addition, regulatory authorities like the FCC, FTC, and the European Data Protection Board will play an important role in ensuring SafeHaven meets data privacy laws. By building strong partnerships with key stakeholders, SafeHaven aims to set a new benchmark in secure, private smart home technology, ensuring that users retain full control over their personal data.

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

To measure the success of our privacy improvements, we will use three main metrics. First, we will track the reduction in cloud storage use. We will collect data for 30 days before and after deploying local voice processing and encryption. Our goal is to reduce cloud reliance by

75%. In addition, we will survey 300 users about their sense of data security, asking them to rate their privacy on a scale from 1 to 10. An average score of 8 or above will indicate that users feel secure.

Next, we will track the security of every interaction by logging whether it is encrypted or not. We will simulate 1,000 interactions under different network conditions to check our encryption system and then continue to collect live data for one month. We expect that at least 95% of all interactions will be encrypted. This approach will help us ensure that our privacy enhancements are working effectively.

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

SafeHaven's use of edge computing for home automation raises ethical concerns, including data privacy, security, and biases in automation. Unauthorized data access or misuse could compromise homeowner privacy, and automatic decision making may introduce biases.

A relevant case is *Carpenter v. United States (2018)*, where the Supreme Court ruled that law enforcement must have a warrant to access cell phone location data [1]. This case also exemplifies the ethical and legal importance of protecting personal data.

➔ *Ethical Impact Risk Table:*

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights
Homeowners	Low	High	Mid	High
SafeHaven	Mid	Low	High	Low
Regulators	Low	Low	Mid	Mid

Homeowners: Low financial risk but high privacy risk due to the data collection. There's a mild conflict between convenience and privacy. High risk of rights violation if data is misused.

SafeHaven: Moderate financial risk from legal and functional costs. Low privacy risk as data is stored locally, but high conflict between business goals and ethical responsibility. Low risk of rights violation with proper security.

Regulators: Low financial risk but mild conflict between consumer protection and innovating. Minimal privacy concerns because of legal oversight, but rights violations could happen if data laws are not followed.

1.C.1.4 OKR 1 Ethical Safeguard

To protect user privacy and avoid biases in data handling, Sentinel Sphere Inc. will take steps to ensure users are fully informed about how their data is being used. This includes providing clear consent forms and real time notifications whenever data is being processed. Also, we will ensure our AI systems are trained on diverse datasets to prevent any bias. We'll work with privacy experts, cybersecurity specialists, and ethical specialists to create and implement these safeguards. We will measure the effectiveness of these safeguards through user feedback to make sure data is secure and our users trust the system. These steps align with ethical guidelines from IEEE, which focus on the importance of adhering to ethical standards in AI systems [2].

1.C.2.1 OKR 2 Objective and Key Result

OKR: Launch a data access dashboard that allows users to review, manage, and delete their data, with at least 30% of active users interacting with it within the first three months.

Our upcoming data access dashboard lets users review and control their personal

information while ensuring transparency and complete user control. The initiative aims to boost regulatory compliance while building consumer trust and enabling users to manage their data conveniently. Our measure of success will be based on adoption rates with the target of getting at least 30% of active users to use the dashboard during its first three months on the market. We strive to boost user transparency through data management optimization and user accessibility while following rules like the CCPA and GDPR.

Our users represent the essential stakeholders for this OKR because they directly benefit from this feature's implementation. The users of our service include people who value their privacy together with digital consumers and tech-savvy individuals who require clear transparency from their online services. This demographic consists of people between 18 and 45 years old who represent multiple genders and races and demonstrate significant concern for data security and online privacy. The dashboard will give these users enhanced control of their personal data but its effectiveness depends on how user-friendly it is. If the interface appears overly complex or lacks clarity it will result in user frustration and reduce both adoption rates and engagement levels.

The introduction of this OKR has substantial internal implications for our product development process, engineering operations, and legal compliance requirements. The product and engineering teams must design and implement the dashboard so that it integrates smoothly into the platform while users get straightforward privacy controls. Challenges associated with this requirement involve real-time data deletion and retrieval without causing system performance disruptions. The legal and compliance teams will maintain compliance with privacy laws and verify that the dashboard meets regulatory requirements. The system must adapt to global regulations due to varying privacy laws across different jurisdictions and it needs to pass

the evaluations made by watchdog organizations.

External stakeholders include governments and regulatory bodies such as the Federal Trade Commission (FTC) and European Data Protection Authorities which maintain significant importance. These organizations monitor business compliance with privacy laws and have the authority to conduct audits or issue penalties to businesses that do not allow users sufficient data control. The Electronic Frontier Foundation (EFF) and consumer rights organizations will oversee the dashboard's performance and advocate for changes if it fails to adequately meet user Needs.

These stakeholders have highly interdependent relationships. Users demand privacy tools from the company which needs to align between user demands and regulatory standards with its business goals. Privacy advocacy groups together with government agencies monitor companies to ensure they fulfill their stated commitments. This OKR goes beyond compliance to establish a benchmark for transparency and user control which builds trust and demonstrates our commitment to responsible data management.

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

Objective: Ensure transparency and user control over data.

Key Result: Release the data access dashboard which permits users to examine their information and execute changes or removals while achieving user interaction by at least 30% of active users during the initial three months.

We will measure this OKR's success by tracking various performance indicators through

structured experiments that provide necessary data. Experiments will assess user adoption rates and test usability and sentiment about the data access dashboard.

Metric 1: User Adoption Rate

Definition: Percentage of active users who interact with the dashboard in the initial three months following its release

Experiment: User Interaction Tracking

Objective: Measure how many users access the dashboard and perform at least one meaningful action (reviewing, managing, or deleting data).

Implementation Steps:

1. Set up analytics tracking in the dashboard to record interactions, including:
    - Clicking on the data access dashboard.
    - Reviewing stored personal data.
    - Editing or deleting data.
    - Completing a session in the dashboard.
2. Define an active interaction threshold to consider meaningful engagement. For example, a user should perform at least one of the following:
    - Spend at least 1 minute on the dashboard page.
    - View at least two different sections of their data.
    - Modify or delete at least one data entry.
3. Compare adoption rates over time by tracking the percentage of users engaging with the dashboard weekly and monthly.

Success Criteria:

• At least 30% of active users should engage with the dashboard in the first three Months.

• A gradual increase in usage over time indicates growing user trust and adoption.

Metric 2: Usability and User Satisfaction

Definition: Users' satisfaction with the dashboard's functionality, ease of use, and usefulness.

Experiment: User Satisfaction Survey & Usability Study

Objective: Measure how easy and useful users find the dashboard through direct feedback.

Survey Implementation:

• Sent to all users who interact with the dashboard.

• 5-question survey using a Likert scale (1-10).

• Open-ended feedback options to capture qualitative insights.

Survey Questions:

1. On a scale of 1-10, how easy was it to find and use the data access dashboard?

2. Did you find the dashboard helpful in managing your data? (Yes/No)

3. On a scale of 1-10, how satisfied are you with the control this dashboard gives you over your data?

4. Would you recommend this feature to others who are concerned about privacy? (Yes/No)

5. What improvements would you suggest for making the dashboard more user-friendly? (Open-ended response)

Usability Study Implementation:

• Recruit 20-50 users to complete specific tasks using the dashboard while being Observed.

• Tasks include:

• Locating their stored personal data.

• Deleting specific entries.

• Understanding how to retrieve deleted data (if applicable).

• Record time taken and any confusion/frustration points.

Success Criteria:

• Average satisfaction score of 8/10 or higher from survey responses.

• At least 80% of usability study participants complete tasks successfully without outside help.

Metric 3: Retention & Continued Usage

Definition: Percentage of users who revisit the dashboard to manage their data after their initial interaction.

Experiment: Engagement & Return Rate Analysis

Objective: Determine whether users continue to use the dashboard over time, rather than interacting once and forgetting about it.

Implementation Steps:

1. Track repeated usage of the dashboard at 30-day and 90-day intervals.
2. Segment users based on behavior:
    - One-time users (used the dashboard once and never returned).
    - Occasional users (returned at least once within 90 days).
    - Frequent users (used the dashboard more than twice within 90 days).
3. Monitor behavior patterns to see if there are spikes in usage when privacy concerns arise in the news (indicating increased trust in our platform).

Success Criteria:

- At least 50% of initial users return within 90 days to review or manage their data.
- A gradual increase in repeat usage indicates long-term adoption rather than one-time curiosity.

Metric 4: Regulatory & Compliance Adherence

Definition: Ensuring the dashboard meets all legal requirements and avoids regulatory penalties.

Experiment: Compliance Audit & Legal Review

Objective: Verify that the dashboard complies with GDPR, CCPA, and other data privacy laws.

Implementation Steps:

1. Conduct an internal compliance audit with legal experts to review dashboard functionality.
2. Run a simulated regulatory review to identify potential risks before an official audit.
3. Monitor for complaints or legal inquiries related to the dashboard's effectiveness in

providing data transparency.

Success Criteria:

- 100% compliance with data protection laws.
- Zero regulatory warnings or fines within the first year of implementation.

Conclusion

The evaluation of user adoption together with satisfaction levels, retention rates, and compliance will determine the success of the data access dashboard in achieving its intended purpose. Behavioral data together with user feedback and compliance testing creates a framework where success becomes measurable and actionable while meeting both user needs and regulatory demands.

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

The data access dashboard allows users to control their personal information by enabling effective management through transparent systems which build trust. Privacy protection concerns alongside data security protocols user accessibility standards and regulatory compliance requirements present numerous ethical considerations. Data autonomy through this initiative poses ethical risks when implementation problems occur or when business needs to oppose security protocols.

The possibility of user data being misused or mishandled represents a significant ethical issue even when users can access their data using a transparent dashboard. Users may believe their data is completely deletable but data copies and metadata often remain in backup systems and

third-party databases. The Facebook–Cambridge Analytica scandal demonstrated how users' data remained accessible for political targeting even after users believed it was deleted [3]. The situation demonstrates that data access systems with good intentions may still be inadequate at stopping unethical data storage and misuse.

Potential Ethical Scenarios

1. **Data Retention After "Deletion"**

    • Users may think they have erased their data but backup versions or mandated records will often remain. Users develop a misplaced sense of security about their data which eventually leads to distrust in the platform [4].

    • Any unauthorized access to this data by third parties may lead to financial losses, legal consequences, or reputational damage for the user.

2. **Unclear or Complex Dashboard Interface**

    • A challenging dashboard navigation experience prevents users from efficiently finding and deleting their data. The difficulty of navigation would create an uneven burden on those who are not proficient with technology while highlighting existing issues in accessibility and digital literacy.

    • When an interface is poorly designed it functions as an intentional dark pattern that stops users from accessing all their data management options.

3. **Conflicts of Interest in Data Accessibility**

• The company may have a financial incentive to **retain user data for analytics, advertising, or business insights**, even after users request deletion.

• If the business prioritizes **profit over privacy**, it may introduce policies that **make full data deletion difficult**, requiring multiple steps or long waiting periods.

4. **Third-Party Data Sharing Risks**

• Even if the company ensures user control within its system, **third-party integrations** (e.g., advertisers, data partners) may have already stored the data.

• Users might **delete their data** from the platform but **unknowingly leave copies in external databases**, leading to ongoing privacy risks.

Expected Ethical Impact Risk Table

Stakeholder	**Financial** Risk	**Privacy** Risk	**Conflicting Interest Risk**	**Violation**
Users (Customers)	Low	High	Low	High
Company (Product & Engineering)	High	Low	Mid	Low

Company (Legal & Compliance)	Mid	Low	High	Low
Government & Regulators	None	Low	Mid	None
Privacy Advocacy Groups	None	Mid	Mid	None

Analysis of Ethical Impact Risk by Stakeholder

Users (Customers):

• **Financial Risk (Low):** Users do not incur **direct financial costs** for accessing the dashboard, but indirect costs could arise if privacy breaches lead to **identity theft, fraud, or loss of personal reputation**.

• **Privacy Risk (High):** Users may expect **full control over their data**, but limitations in deletion policies, third-party data retention, or unclear policies could **undermine their privacy**.

• **Conflicting Interest Risk (Low):** Users generally have a **unified interest** in controlling their data, though some may prioritize convenience over privacy.

• **Violation of Rights Risk (High):** If the dashboard fails to **fully delete data** or **misleads users**, it could violate data protection laws like GDPR and CCPA, affecting users' legal rights.

Company (Product & Engineering Teams):

• **Financial Risk (High):** Implementing a transparent **data access dashboard requires resources**, potentially reducing revenue from **data-driven insights and ad targeting**.

• **Privacy Risk (Low):** The technical teams focus on compliance, but **unintentional security flaws** or poor UX design could still expose privacy risks.

• **Conflicting Interest Risk (Mid):** The company may face **internal pressure** to balance privacy commitments with **business growth strategies that rely on user data**.

• **Violation of Rights Risk (Low):** If the dashboard meets **legal standards**, rights violations should be minimal, but **compliance gaps** could lead to future legal disputes.

Company (Legal & Compliance Teams):

• **Financial Risk (Mid):** Legal teams **incur costs** for ensuring regulatory compliance and mitigating legal risks, though **avoiding lawsuits or fines outweighs short-term costs**.

• **Privacy Risk (Low):** Compliance teams work to **ensure privacy standards**, but lack of company-wide enforcement could lead to unintentional breaches.

• **Conflicting Interest Risk (High):** Legal teams may face **pressure from executives** to interpret laws **in ways that favor the business**, even if it weakens user privacy.

• **Violation of Rights Risk (Low):** If legal teams enforce **strong compliance measures**, direct rights violations should be **minimized**.

Government & Regulatory Bodies:

• **Financial Risk (None):** Governments do not bear **direct financial costs** from company privacy policies.

• **Privacy Risk (Low):** Regulatory agencies may **miss violations** or fail to enforce policies effectively.

• **Conflicting Interest Risk (Mid):** Regulators must **balance industry growth with consumer protection**, leading to **inconsistent enforcement of data laws**.

• **Violation of Rights Risk (None):** Governments do not **directly violate rights** but may fail to **protect users from corporate overreach**.

Privacy Advocacy Groups:

• **Financial Risk (None):** These groups are typically **nonprofit and not financially impacted**.

• **Privacy Risk (Mid):** If the company fails to **fully comply with privacy laws**, advocacy groups may **face challenges exposing** these violations.

• **Conflicting Interest Risk (Mid):** Some privacy groups **receive funding from industry players**, creating **potential conflicts of interest** in their advocacy efforts.

• **Violation of Rights Risk (None):** Advocacy groups seek to **prevent rights violations** rather than commit them.

Conclusion

A data access dashboard presents ethical challenges that necessitate a careful equilibrium among business interests and both transparency and privacy concerns. The initiative encourages user control but faces possible effectiveness challenges from incomplete deletion processes, poor accessibility features, and potential conflicts of interest. The Facebook–Cambridge Analytica scandal demonstrates that companies need to take active measures against deceptive data practices to steer clear of ethical mistakes. The company achieves maximum ethical standards and regulatory compliance by focusing on usability together with legal compliance and robust data deletion protocols.

1.C.2.4 OKR 2 Ethical Safeguard

To minimize the ethical risks associated with privacy, transparency, data retention, and conflicting interests, we must establish effective safeguards to ensure the dashboard genuinely empowers users while maintaining compliance with privacy laws. These safeguards will be

designed and implemented with the help of privacy experts, UX designers, regulatory advisors, and user research groups to ensure effectiveness.

Safeguard 1: Full Data Deletion Confirmation & Transparency Logs

Description & Implementation

Users face significant ethical risks when they delete their data but remnants remain in backups and third-party databases. True transparency requires the dashboard to feature:

1. **Clear Confirmation & Timeframe for Deletion**

    • Users receive a complete summary of their deletion action including the details of deleted content and storage locations as well as the backup removal timeframe.

    • Example: The system has planned permanent removal of your account data. The data will be eliminated from every system and backup storage within a 30-day timeline. Users have the ability to ask for documentation related to this deletion procedure.

2. **Data Deletion Transparency Log**

    • Users can review their personalized data deletion log which displays the status of their past deletion requests and system processing progress.

    • This ensures users understand data deletion takes time due to legal and technical constraints instead of appearing to be immediate.

Who Designs It?

• **Privacy Law Experts & Compliance Officers** → Ensure the process aligns with **GDPR, CCPA, and other data protection regulations**.

• **UX/UI Designers & Human Factors Experts** → Design a dashboard that **communicates the deletion process without technical jargon**.

• **Software Engineers & Data Security Experts** → Implement a **secure method to log and display deletion status**.

How to Measure Effectiveness?

• **Surveys** asking users if they felt **fully informed** about their data deletion.

• **Audit reports** verifying that all requested deletions were carried out correctly.

• **Legal compliance checks** ensuring adherence to data protection laws.

Safeguard 2: Accessibility-Optimized Dashboard with Dark Pattern Prevention

Description & Implementation

A poorly designed dashboard may unintentionally (or intentionally) discourage users from managing their data, leading to **ethical concerns around accessibility and user autonomy**.

1. **Simplified Navigation & Accessibility Testing**

• The dashboard will feature **clear, easy-to-understand labels** with **no hidden settings**.

• Every data management option will be **accessible within three clicks** to avoid burying important settings.

• **Accessibility testing** will ensure usability for **individuals with disabilities** (e.g., screen reader support, high-contrast mode).

2. **Prohibiting Dark Patterns**

• Design choices that **intentionally confuse or manipulate users** (such as misleading button placement or default settings that retain data) will be banned.

• Example: The **"Delete My Data"** button will be **equally prominent** as the "Cancel" button, preventing deceptive design.

Who Designs It?

• **UX/UI Designers & Behavioral Scientists** → Ensure the dashboard is **intuitive and free of deceptive patterns**.

• **Accessibility Experts (e.g., WCAG Compliance Specialists)** → Validate usability for **visually impaired and disabled users**.

• **User Testing Groups** → Gather feedback from **diverse demographics**, ensuring fairness in design.

How to Measure Effectiveness?

- **A/B Testing:** Users are given different versions of the dashboard to see which leads to higher engagement.

- **User Satisfaction Ratings** from accessibility audits.

- **Dark Pattern Compliance Review** conducted by an external **ethics panel**.

Safeguard 3: Independent Privacy Audits & Public Reporting

Description & Implementation

To **build trust and prevent regulatory violations**, the company will **commit to independent, third-party privacy audits** and **public transparency reports** outlining data retention and deletion practices.

1. **Annual Third-Party Privacy Audits**

    - External **privacy consultants** will review whether the dashboard **fully complies** with laws like **GDPR and CCPA**.

- Any violations or oversights must be **corrected within 60 days**.

2. **Public Transparency Reports**

- Biannual **reports detailing** how many deletion requests were made, how long deletions took, and **if any regulatory complaints were received**.

- Users should be **able to see aggregate statistics** without exposing personal details.

Who Designs It?

- **Independent Privacy Firms** (e.g., Electronic Frontier Foundation, Mozilla Privacy Lab) → Conduct audits.

- **Regulatory Advisors** → Ensure **full compliance** with local and international laws.

- **Ethics Committees & Watchdogs** → Provide **oversight to prevent corporate bias**.

How to Measure Effectiveness?

- **Audit Scores & Regulatory Compliance Reports** (Pass/fail based on laws).

- **Public Trust Surveys** measuring whether users feel confident in the company's privacy efforts.

- **Government Enforcement Actions** (e.g., no fines or violations).

Safeguard 4: User-Controlled Data Sharing with External Entities

Description & Implementation

Even if users delete their data, **third-party advertisers and data brokers may have already accessed copies**. To prevent this, users should be able to **see and revoke data access** to external parties **in real-time**.

1. **External Data Sharing Visibility Panel**

• A **dashboard section listing all third parties** that have accessed user data.

• Users can **revoke access instantly**, preventing further sharing.

    • Example: "Your data has been accessed by [Company X] for analytics. Click here to revoke future access."

2. **Data Request History & Reversal**

    • Users should be able to **download a record** of their shared data and request **removal** from external entities.

Who Designs It?

• **Data Protection Lawyers** → Ensure compliance with **third-party data regulations**.

    • **Cybersecurity & Software Engineers** → Develop **secure access controls** for real-time revocation.

• **User Advocacy Groups** → Ensure **users understand their rights** and available options.

How to Measure Effectiveness?

• **Percentage of users who successfully revoke third-party access** after first viewing the panel.

• **Legal complaints** related to unauthorized third-party sharing.

• **Survey responses** measuring user confidence in external data visibility.

Conclusion

The safeguards decrease ethical risks through enhanced data transparency and accessibility while granting users better control of their personal information. Abuse prevention and unintended consequences mitigation require ethical design principles as well as external accountability and privacy-first policies. The implementation of these safeguards ensures adherence to GDPR, CCPA, and IEEE ethical standards while lowering potential legal breaches and diminishing user distrust [5].

1.C.3.1 OKR 3 Objective and Key Result

SafeHaven aims to help homeowners and renters reduce their energy consumption by 15% monthly through the use of smart home automation. This will be done via the integration of smart meters, smart switches, and as well as smart thermostats powered by the SafeHaven home assistant. Energy usage remains a concern for homeowners as energy consumption increases, so will the energy bills. We want to empower homeowners with reasonable insights and automated solutions that will be cost saving in the long run. These energy saving solutions will especially be beneficial for lower to middle income families to reduce some financial stress and to allow more focus on other essential needs. These tailored solutions will be based on data collected on daily activities and usage based on the type of household, families with children, and for the elderly who will benefit from an automated energy management system to accommodate their needs. As data is being collected, our security experts will work to maintain that the data remains secure and private. This tailoring will directly address the needs of diverse demographics, ensuring that energy-saving measures are both effective and convenient for all users.

With the use of smart meters, SafeHaven will be able to collect the data through the smart meters provided by the energy companies and work with our team of data analysts, AI specialists, and software engineers to create these personalized y use reduction recommendations. With this, homeowners would have the ability to choose between implementing it manually or through automation via SafeHaven. This flexibility gives homeowners and renters the ability to review and adjust accordingly or to have a hands-free automated energy management system. Additionally, we will seek feedback from our customers to ensure that SafeHaven is efficiently accommodating and accessible. Ultimately, we want SafeHaven to be utilized as an energy saving tool for our customers for cost savings that is also accommodating based on personal needs that is comfortable for the customers.

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

In order to test for a 15% reduction in energy consumption powered by SafeHaven, Sentinel Sphere will look to have 300 households participate in this experiment, ranging from low to middle income families, households with children, and the elderly. The participating households will act as the control group and also as the experimental group.The primary unit of measurement here will be kilowatt-hours (kWh) as it is the standard to measure electricity usage over a certain period of time. In this first experiment, it will set a baseline period in which the first step would be to collect energy usage data of the participating households, pre-implementation of SafeHaven's features. This includes data collected from smart thermostats and smart switches by smart meters. The participating households will act as the control group and also as the experimental group. Once the data is collected, the data will be collected and analyzed as the baseline measurement. After the baseline period, then comes the automation period, the implementation of SafeHaven. With the data collected from the baseline period, SafeHaven will use that data and be able to provide each household their own automated tailored energy saving recommendations. Once the automation period is over, our team of analysts and engineers will look to see if SafeHaven's energy optimization features have in fact helped reduce energy consumption by 15% monthly.

In addition to our main objective of a 15% energy use reduction, we will also look at the cost savings of using SafeHaven's energy optimization features. To do this, we will look at the first experiment and look at the difference in energy consumption of the before and after implementation of SafeHaven. To measure the cost of savings, we will have to look at the

difference in energy usage before and after SafeHaven. Once the difference is found, multiply the difference by the unit price per kWh. Assuming a 15% reduction in energy use is met, an example would be 800 kWh used before SafeHaven would be 680 kWh post SafeHaven. The difference in that would be 120 kWh and by multiplying that by the price per unit of kWh which could be $0.15. That gives you $18 and multiply that by 12 months and it would be an annual cost savings of $216. This just gives an idea of how SafeHaven would help reduce and optimize energy usage while also saving money in the long run.

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

As SafeHaven implements its smart home automation system to reduce energy consumption by 15%, there are some ethical concerns regarding data privacy, financial implications, and conflicts of interest. As smart home automation offers cost-saving benefits and increased energy efficiency, it also involves the collection of household data which can be sensitive. As a result, one of the main concerns is the privacy and security of that data. SafeHaven collects energy usage data from smart meters, smart switches, and thermostats to tailor recommendations, but if this data is not securely handled, it could be sold to third parties or used to manipulate consumer behavior. In recent news, Apple has agreed to pay $95 million to users that have had their conversations captured by Siri and potentially heard by employees. Also, initial claims stated that Apple let advertisers use these captured recordings to target users to develop a marketing profile on them [6]. This is a major concern because people should not have to worry about moments of their daily lives being captured, they should be able to trust that their conversations and moments be private and secure. Smart thermostats collect data in which most consumers don’t realize. Data collected which can be collected include temperature

settings, environmental information, and other seemingly harmless information can be leveraged to third parties for marketing purposes [7]. As a result of this, there will be many ads that pop up when you open up your phone, device, or laptop based on the data collected and if shared.

We will work to ensure that the data remains private and secure to prevent this from happening, ensuring trust with our consumers. Additionally, financial and conflicting interest risks must be considered. With the partnership with energy companies, we understand that this could create conflicts of interest if SafeHaven's energy optimization features benefit the consumers over the companies in which energy usage is reduced, there could be a potential drop in profit for the energy companies. We will work to ensure that both parties are satisfied with their respective concerns.

Expected Ethical Impact Risk Table

Stakeholder	**Financial**	**Privacy**	**Conflicting Interest**	**Violation of Rights**
Homeowners/renters	Mid	High	Low	Mid
Sentinel Sphere	Mid	Mid	High	Mid
Cybersecurity Experts	Low	Low	Low	Low
Software Engineers	Low	Mid	Low	Low
AI Specialists	Low	Mid	Low	Low
Data Analysts	Low	Mid	Low	Low
Energy Companies	Mid	Mid	Mid	Mid

Homeowners/renters: The financial risk is low because SafeHaven's primary goal is to reduce energy consumption and associated costs. Though, unexpected algorithmic errors or hidden fees from energy provider partnerships could create hidden expenses in which it is important to maintain transparency. Privacy risk is high because smart home devices collect detailed energy usage patterns which if mishandled or accessed by third parties could lead to targeted marketing profiles. The conflicting interest risk is mid-level because energy providers may have incentives that do not fully align with cost savings for consumers, potentially leading to recommendations that benefit providers over users. Violation of rights risk is mid since there is potential for data privacy violations if proper security safeguards are not maintained.

Sentinel Sphere: Company faces a mid-level financial risk because ethical breaches, such as data misuse or biased algorithms, could lead to lawsuits, fines, and reputational damage, impacting their financial stability. There is also the financial impact of manufacturing the SafeHaven device. They face a mid-level privacy risk as the handlers of sensitive user data, making them vulnerable to significant repercussions from data breaches. They have a high conflicting interest risk due to the possibility of monetizing user data which creates a conflict between profit motives and the responsibility to protect user privacy. They face a mid-level violation of rights risk because their actions, such as data misuse or discriminatory algorithm deployment, could directly violate users' rights to privacy, equal treatment, and autonomy.

AI Specialists, Software Engineers, and Data Analysts: The financial risk is low as their employment is related to SafeHaven's long-term success. Privacy risk is mid because they will have access to sensitive user data for analysis and system improvements, and any mismanagement or leaks could lead to significant concerns. Conflicting interest risk is mid, as data analysts may face some pressure to optimize recommendations in ways that would favor energy providers slightly over consumers. Violation of rights risk is low, since they are expected to follow ethical guidelines.

Cybersecurity Experts: The financial risk is low, as their job security is to maintain SafeHaven's strong security measures. Privacy risk is low since their role is to protect user data rather than access it. Conflicting interest risk is low, as cybersecurity experts are primarily focused on security and compliance. Violation of rights risk is low because their primary function is to safeguard user data and uphold privacy protections.

Energy Companies: They face a mid-level financial risk because changes in energy consumption patterns driven by SafeHaven could potentially impact their revenue. They face a mid-level privacy risk as they share sensitive customer data with SafeHaven, creating a risk of data breaches or misuse which requires careful handling of data. They have a mid-level conflicting interest risk as there is the issue of balancing their profit and having the responsibility to provide reliable and affordable energy. They face a mid-level violation of rights risk because misuse of data or the creation of unfair access to energy could violate consumer rights to privacy and equal treatment.

1.C.3.4 OKR 3 Ethical Safeguard

One of the primary concerns is the collection and handling of sensitive user data, including energy consumption patterns and device usage. One of the ways we will work to mitigate the issue is to implement end-to-end encryption and edge computing. Edge computing has emerged as a way to ensure a higher sense of data security by reducing the amount of data transmitted to outside servers such as the cloud [8]. In order for this to be achieved, our team of specialists and engineers will work to implement these features in order for our customers to feel more at ease with how their data will be handled. With this, it would also reduce the amount of third party eyes on the data that lead to endless marketing advertisements. Effectiveness will be measured by monthly security audits, searching for data breaches, and surveys for customers regarding data privacy policies and practices. In addition, having an ethics review board would allow for independent eyes on data policies, review algorithmic fairness audits, and address ethical concerns raised by users. The board will consist of legal experts, advocates for consumers, tech experts, and ethicists. The board will be able to review policies and ethical concerns to provide recommendations in improving these ethical safeguards through review meetings regarding SafeHaven. In order to measure the effectiveness of the ethics review board, there will be an audit on tracking ethical issues raised by the board and to take necessary actions regarding the issues as well as surveying the public view of SafeHaven's data policies. With these safeguards in place, we want to ensure security and privacy of consumer data.

1.C.4.1 OKR 4 Objective and Key Result

Sentinel Sphere Inc. aims to establish the SafeHaven (SH) smart home assistant as a top contender in the smart home industry. By incorporating advanced natural language processing (NLP) and predictive processing, SH seeks to reduce incorrect command executions by 20% while improving response times by 25%. These enhancements will create a more seamless user experience, increasing customer satisfaction and engagement. Additionally, SH prioritizes privacy through edge computing, minimizing reliance on cloud storage and addressing common data security concerns.

Key stakeholders include homeowners, renters, and energy companies, each with unique interests in SH's capabilities. Homeowners and renters highly value privacy and security, making SH's local data processing a crucial trust-building feature. Cybersecurity experts play a critical role in protecting SH from potential threats, reinforcing its reputation as a secure and reliable device. Meanwhile, energy companies contribute by integrating smart switches that promote energy efficiency, appealing to environmentally conscious users and those seeking to lower energy costs. This collaboration ensures SH remains at the forefront of smart home technology, balancing functionality, security, and efficiency for a wide range of users.

1.C.4.2 OKR 4 Metric(s) with Experiment(s)

To measure the success of the OKR for SH, key metrics will focus on command accuracy, response time, and user satisfaction. One essential metric is command execution accuracy with the goal of reducing incorrect executions by 20%. This will be measured by analyzing the rate of successful command responses versus logged errors. An experiment to test this metric would track 100 user interactions with SH across a diverse demographic, including age and gender,

over a month. The data collected will categorize errors by type (misinterpretation, system failure) to refine improvements.

Another crucial metric is system responsiveness with the objective of improving response time by 25%. This will be assessed by tracking the average processing time for SH to execute user commands. The experiment will simulate various network conditions to evaluate latency and understand how edge computing impacts processing speed.

For user satisfaction, a post-interaction survey will be conducted. The survey will include questions such as: On a scale of 1-10, how satisfied were you with the system's response time? and how easy was it to control your devices through SH? These metrics will provide quantitative and qualitative insights, ensuring continuous improvement of the product.

1.C.4.3 OKR 4 Ethical Impact(s)/Issue(s)

Despite the potential benefits, there are various ethical impacts and issues that may arise during the development and use of the system.

- Data Privacy and Security: Possibility of vulnerabilities within the local devices or during the data transmission process remains, sensitive user information such as personal preferences, voice data could be compromised.
- Potential Ethical Scenario: Users may unknowingly expose sensitive data if there is a flaw in the encryption this can lead to a breach of user trust.

a. **Expected Ethical Impact Risk Table**

Stakeholder	Financial Risk	Privacy Risk	Conflicting Interest Risk	Violation of Rights

Homeowners/Renters	Low	High	Medium	High
Energy Companies	Low	Low	High	Low

b. **Analysis of Ethical Impact Risk**

Homeowners/Renters as Stakeholders: Homeowners and renters are not likely to face direct financial risks from purchasing the system or paying subscription fees. However, their privacy risk is high due to the collection of sensitive personal data. A breach in data security could lead to severe privacy violations. Additionally, there is a conflicting interest risk if developers prioritize functionality over privacy. If users are unaware of the extent of data collection, their privacy rights could be violated. "Apple employed contractors to listen to Siri recordings of private conversations, including medical appointments, sexual encounters, and drug deals" [9].

Companies as Stakeholders: Companies do not face direct financial risks from data breaches or privacy concerns related to SH. Their privacy risk is low because they do not have direct access to sensitive user data. However, conflicting interest risk is high since companies may collect data to improve operations. The risk of violating user rights is low because they do not handle user data in ways that would directly infringe on privacy rights.

1.C.4 .4 OKR 4 Ethical Safeguard

Ensuring privacy and security in the SH smart home assistant is a key goal. The main ethical concern is data privacy and security risks, as smart home assistants handle sensitive user information. To protect this data, Sentinel Sphere Inc. will use local data processing with edge computing and end-to-end encryption.

One important safeguard is edge computing, which processes data locally instead of sending it to external servers. This reduces the risk of cyber threats and improves privacy. In addition, end-to-end encryption will secure all data transmissions to prevent unauthorized access. SH will also include a privacy dashboard that allows users to review, manage, and delete their data easily.

The effectiveness of these safeguards will be evaluated through penetration testing, user feedback surveys, and data breach monitoring. These methods will help ensure that the safeguards remain strong and continue to improve over time, making SH a reliable and efficient smart home assistant.

2: Cultural Policy

2.A. Core Values

At Sentinel Sphere Inc., our core values serve as the foundation of every innovation, decision, and interaction we engage in. We want to be thought of as the pioneers of ethical AI-driven home technology—leaders who never compromise user trust in pursuit of advancement. At the heart of our culture is Privacy First. We believe that no innovation is meaningful unless it protects the personal boundaries and autonomy of those it serves. Our commitment to Transparency ensures that every user knows exactly how their data is used, stored, and protected. User Empowerment fuels our design philosophy—we do not just build technology; we craft tools that give individuals more control over their environment and lives. Innovation with Responsibility guides our technical exploration, ensuring that progress never comes at the cost of security, ethics, or sustainability. Lastly, Sustainability is more than an add-on; it is a core responsibility. Our products are designed not only to make homes smarter but

to make the planet greener through intelligent energy-saving practices. These values shape a company that refuses to settle for the status quo and actively redefines what ethical, smart living should look like.

2.B. Motivation

What drives Sentinel Sphere Inc. is to develop technology that truly serves people not corporations, not algorithms, but real, everyday individuals. We want to develop intelligent systems that will improve lives while keeping boundaries in mind. We are passionate about helping people feel safe, understood, and in control within their homes. Our passion comes from solving hard problems ethically, from developing AI that doesn't just work efficiently but does so while honoring the user's right to privacy and transparency.

What we fear is becoming what we set out to challenge. We fear a future where convenience overshadows privacy, where smart technology becomes synonymous with surveillance. We are wary of trends that prioritize profit over ethics, and we are constantly vigilant against the temptation to cut corners or compromise our values. This fear does not paralyze us; instead, it pushes us to be more thoughtful, more innovative, and more transparent. It reinforces our belief that ethical technology is not just possible—it is necessary.

2.C. Summary

Privacy. Empowerment. Ethics. Innovation. Sustainability.

3: Ethics Policy

3.A. Core Items

At Sentinel Sphere Inc., our ethics policy is the backbone of our operations, product development, and company culture. It ensures our technologies serve people with integrity, fairness, and accountability. Each core item of this policy outlines the principles and actions we uphold across all departments.

1. Privacy by Design

We build privacy into the architecture of every system we create. Our smart home assistant, SafeHaven, uses edge computing to process data locally, minimizing cloud reliance. This ensures that users retain full ownership of their personal information. We never collect, sell, or share user data without explicit consent. Privacy is not optional—it's a default feature.

2. Transparency and Informed Consent

Every user has the right to understand how SafeHaven works and what data it processes. We commit to providing plain-language disclosures, easy-to-access settings for managing data, and detailed logs for user review. We also prohibit dark patterns—design choices that manipulate users into actions they wouldn't otherwise take.

3. Ethical AI Development

Our AI algorithms are designed to avoid bias, respect context, and respond safely. We evaluate all models for fairness, accuracy, and non-discrimination. We consider the broader

social impact of our systems, particularly around surveillance, autonomy, and trust. We avoid opaque black-box systems unless explainability can be guaranteed.

4. Sustainability and Environmental Responsibility

We are committed to reducing environmental impact through responsible sourcing, manufacturing, and product design. SafeHaven includes energy monitoring features that encourage lower consumption and emissions. Our company supports circular economy principles: minimizing e-waste and offering repairable, upgradeable hardware.

5. Fair Labor and Inclusion

We recognize the many forms of labor that go into AI and smart tech development—from engineers to testers to data markers. We commit to fair wages, safe working conditions, and diverse hiring practices across gender, race, and background. We ensure inclusion not only in the workplace, but in how our products serve diverse communities.

6. Accountability and Oversight

We establish internal and external ethics oversight through regular audits, user feedback loops, and an independent advisory board. Any ethical breaches or misconduct will be transparently addressed. We invite researchers and watchdogs to critique our systems and we are open to making changes in response.

3.B. Board

1. Dr. Latanya Sweeney

Dr. Sweeney is a professor of Government and Technology at Harvard Kennedy University and former Chief Technology Officer at the U.S. Federal Trade Commission. Her groundbreaking work in data privacy, including re-identification of anonymized datasets, makes her a global authority on digital ethics. We chose her because of her experience in privacy protection, data governance, and ethical technology deployment which aligns well with SafeHaven's goal to secure user data through local processing and encryption.

2. Bruce Schneier

Bruce Schneier is a well known cryptographer and cybersecurity expert and is currently a lecturer in Public Policy at the Harvard Kennedy School. He has written several books on computer security and has advocated for the ethical development of technology. His deep expertise in encryption, security architecture, and policy makes him an essential voice on our board. With his guidance, we can ensure that SafeHaven stays resilient against external threats while maintaining transparency, efficiency, and trust.

3. Dr. Timnit Gebru

Dr. Gebru is the founder of the Distributed AI Research Institute (DAIR) and a strong voice in the AI ethics community. Her research focuses on algorithmic bias, ethics in large-scale machine learning, and the impact of AI systems on marginalized communities. She has also previously co-led Google's Ethical AI team. We chose her not only for her technical insights but also for her commitment to justice, fairness, and the social implications of AI technology. Having her on the board ensures that our product development considers power dynamics, equity, and real-world consequences.

These three board members will provide Sentinel Sphere Inc. with the ethical, technical, and interdisciplinary expertise necessary to uphold our vision of secure, equitable, and transparent smart home technology.

4: YouTube Presentation

Link to YouTube Presentation of Github Wiki

5: References

[1] 16-402 Carpenter v. United States (06/22/2018), https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf?mod=article_inline (accessed Mar. 3, 2025).

[2] “Autonomous and intelligent systems (AIS) standards,” IEEE Standards Association, https://standards.ieee.org/initiatives/autonomous-intelligence-systems/standards/ (accessed Mar. 5, 2025).

[3] User Data Privacy: Facebook, Cambridge Analytica, and privacy protection, https://www.researchgate.net/publication/327025736_User_Data_Privacy_Facebook_Cambridge_Analytica_and_Privacy_Protection (accessed Mar. 6, 2025).

[4] A contextual approach to privacy online | daedalus | MIT press, https://direct.mit.edu/daed/article/140/4/32/26914/A-Contextual-Approach-to-Privacy-Online (accessed Mar. 7, 2025).

[5] “The IEEE global initiative 2.0 on Ethics of Autonomous and intelligent systems,” IEEE Standards Association, https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/ (accessed Mar. 7, 2025).

[6] A. Robertson, “Apple will pay $95 million to people who were spied on by Siri,” The Verge, https://www.theverge.com/2025/1/2/24334268/apple-siri-recording-privacy-lawsuit-settlement-proposed (accessed Mar. 11, 2025).

[7] G. Drenik, “How data privacy should factor into Your Smart Thermostat Decision,” Forbes, https://www.forbes.com/sites/garydrenik/2023/08/30/how-data-privacy-should-factor-into-your-smart-thermostat-decision/ (accessed Mar. 11, 2025).

[8] A. Prakash, Edge computing to boost security now and in the future, https://pubsonline.informs.org/do/10.1287/LYTX.2025.01.01/full/ (accessed Mar. 11, 2025).

[9] A. Hern, “Apple Contractors ‘regularly hear confidential details’ on Siri Recordings,” The Guardian, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (accessed Mar 10. , 2025).

Group
Members: Yoel Kaleb, Thai Saetern, Kevin Lam, Robert Gutierrez