**User Experience (UX) Research Document**

**1.Objective of Project**

To develop a mobile application that detects, classifies, and evaluates the privacy risks of IoT sensors and trackers in each space. The app will empower users with real-time insights, enhancing privacy awareness and security through risk assessment and mitigation recommendations.

## **2. Research Goals**

* Understand user concerns and pain points regarding digital privacy.
* Design a user-friendly and intuitive app interface for seamless navigation and accessibility.
* Accurately identify and map the location of detected sensors, including distance measurement and room coordinates
* Define technical architecture requirements for privacy implementation.

**3. Participants**

**Target Users:**

* Privacy-conscious individuals who want better control over their digital footprint.
* Professionals handling sensitive data.
* General users who may not be aware of privacy risks but wish to enhance their security.
* Researchers and organizations focused on digital security.

**Sample Size:** 5-10 participants to ensure a comprehensive evaluation.

**Requirements:** Participants should have android smartphones and be willing to test the app in different scenarios.

**4. Research Methodology**

* **Usability Testing:** Conducted usability tests on prototypes to refine UI/UX design.
* **Feedback Collection:** Gathered insights through user testing to refine interface usability and sensor tracking accuracy.

**5. Key Findings**

* **Ease of Use**: Simple and intuitive interfaces encourage user engagement with privacy features.
* **Technical Expectations**: Users expect end-to-end encryption and minimal data retention policies

**6. Key UX Considerations**

* **Welcome Screen -**with a simple and clear "Find Devices" button to initiate scanning.
* **Scanning Phase-** The interface provides a loading animation while scanning for beacon devices.
* **Device List Display -** Users can view detected sensors in a categorized list, making it easy to identify relevant devices.
* **Proximity Awareness -**Displays connected beacons with relevant details, such as name, type, and estimated distance.

**7. Technical Implementation Details**

* **Frontend:** Built with Flutter for cross-platform mobile experiences.
* **Backend:** Developed using Node.js with Express.js for API handling.
* **Database:** Uses AWS DynamoDB for scalable, secure data storage.
* **Sensor Detection:**
  + Detects Beacons using UUID &RSSI signals
  + Utilizes Flutter Blue for BLE beacon detection.

**8. Wireframes & Prototypes**

Low-fidelity prototypes and system architecture diagrams have been developed to test UI workflows and system integrations.

**9. Conclusion**

This UX research provides a strong foundation for developing an effective Privacy Mitigation Tool. By prioritizing user needs, automation, transparency, and security, the application will empower users to take control of their digital privacy with minimal complexity. Future iterations will refine usability and expand features based on ongoing research and feedback.