1. **Purpose**
   This document establishes the approved scope and boundaries of the residential risk management project. It defines which assets and environments are eligible for risk assessment and clarifies exclusions to prevent scope expansion. This baseline serves as the authoritative reference for all project-level risk management activities.

2. **Scope Boundaries**
   This project prioritizes **Confidentiality** and **Availability**, with secondary consideration given to **Integrity**, based on household objectives and risk tolerance.

   - **Confidentiality** focuses on protecting sensitive information such as personally identifiable information (PII) and financial data. While enterprise privacy programs often require regulatory compliance, this project relies on household objectives and risk tolerance as the governing authority.
   - **Availability** addresses resilient access to systems and services required for daily operations and remote work.
   - **Integrity** is considered where unauthorized modification could materially impact financial, personal, or operational outcomes, but it is not treated as a primary driver relative to confidentiality and availability.

   As such, the assets being managed will include devices, systems, services, and personnel commonly found in a residential environment. Anything out of scope is enterprise tooling, employer-managed systems, and continuous monitoring mechanisms typically associated with large-scale environments.