

# Architecture and design

**Goal:** Design an architecture that enforces privacy and security by construction.

1. Produce security architecture diagrams showing trust boundaries, data flows and classification.
2. Apply Data Flow Mapping and Data Classification (sensitive vs non-sensitive).
3. Embed privacy controls: data minimization, consent capture points, and user-facing
4. Specify encryption, key management, segmentation, and secure default configurations.
5. Plan for logging, monitoring, and auditability (what to log, how long, who has access).
6. Document fallback modes and failure behaviors to avoid privacy leaks or insecure defaults.

---

Revision #1

Created 27 November 2025 08:51:18 by RISA

Updated 27 November 2025 08:52:23 by RISA