Core Principles

Combine the foundational Privacy by Design (PbD) principles with Security-by-Design objectives into a unified set:

- **Proactive and preventative:** Anticipate and reduce privacy/security risks before they occur.
- **Privacy and security by default:** Systems must default to the most privacy-preserving and secure configuration.
- **Embedded into design:** Privacy and security are integral to architecture and not bolted on afterwards.
- **Positive-sum functionality:** Achieve privacy and security without unnecessary trade-offs to functionality.
- **End-to-end lifecycle protection:** Protect data across collection, storage, use, transfer, archive, and destruction.
- **Visibility, transparency, and accountability:** Maintain auditability, clear policies, and openness about practices.
- **User-centric and respect for privacy:** Provide clear notices, consent mechanisms, and user controls.
- **Least privilege and segmentation:** Limit access by role and segment networks/systems to reduce blast radius.
- **Continuous improvement:** Monitor, patch, audit, and reassess to adapt to new threats and legal updates.

Revision #1
Created 27 November 2025 08:44:01 by RISA
Updated 27 November 2025 08:45:42 by RISA