

# Minimum Security and Privacy Controls

- Data minimization and purpose limitation, collect only what is necessary.
- Strong encryption for data at rest and in transit; use approved cryptographic standards.
- Role-Based Access Control (RBAC) and Privileged Access Management (PAM).
- Multi-Factor Authentication (MFA) for privileged and remote access.
- Secure-by-default configurations; remove/disable insecure defaults and accounts.
- Secure logging and monitoring with protected audit trails and log retention policy.
- Secure coding standards, code reviews, and static analysis (OWASP, CERT).
- Vulnerability scanning, regular patching and timely security updates.
- Privacy-enhancing technologies where appropriate use pseudonymization and tokenization.
- Network segmentation and least privilege architecture.
- Data retention and secure disposal procedures like sanitization and secure deletion.
- Documented incident response and escalation paths.
- Transparent privacy notices and user consent management.

---

Revision #1

Created 27 November 2025 08:46:09 by RISA

Updated 27 November 2025 08:47:52 by RISA