Scope

What this guideline covers

This guideline applies to all software systems developed, acquired, deployed, or maintained by Government of Rwanda (GoR) institutions. It provides step-by-step instructions, controls, and best practices for embedding privacy and security throughout the software lifecycle, including:

- Software initiation, requirements gathering, architecture and design, development, testing, deployment, operations, maintenance, and decommissioning.
- Risk assessment, threat modeling, and privacy impact assessments (PIAs).
- Implementation of minimum security and privacy controls such as encryption, RBAC, multi-factor authentication, secure coding, vulnerability management, and audit logging.
- Incident management, monitoring, and compliance with Law No 058/2021 (Data Protection) and national minimum cybersecurity standards.

What this guideline does not cover

- Physical security of facilities, data centers, and offices.
- Security of personal devices (BYOD) beyond software access requirements.
- National-level cyber defense operations or military/intelligence systems.
- Vendor internal security policies unrelated to GoR systems.
- Financial, procurement, or project management procedures not related to software security and privacy.
- Non-software systems like manual or paper-based processes.
- User behavior or content moderation on platforms. The focus is on system design and data protection.

Applicable departments and roles

- All GoR institutions developing or using software systems.
- Employees, contractors, and third-party vendors involved in software lifecycle activities.

Revision #1
Created 27 November 2025 09:26:27 by RISA
Updated 27 November 2025 09:28:46 by RISA