Software Security and Privacy by Design Guidelines

This guideline provides practical, step-by-step guidance for embedding security and privacy principles into software development. It aims to ensure that government software systems are secure, resilient, and protect personal data throughout their entire lifecycle.

- Introduction
- Objectives
- Scope
- Target Audience Roles and Responsibilities
- List of Abbreviations
- Core Principles
- Minimum Security and Privacy Controls
- Software development lifecycle step-by-step guidance
  - Initiation
  - Requirements and acquisition
  - Architecture and design
  - Development
  - Testing
  - Deployment
  - Operations and Maintenance
  - Upgrade / Decommission
- Security Incident Management

- Awareness, Training and Best Practices
- Compliance, Audit and Continuous Improvement
- References

Introduction

This guideline provides practical, step-by-step guidance for embedding security and privacy principles into software development. It aims to ensure that government software systems are secure, resilient, and protect personal data throughout their entire lifecycle.

With increasing digitalization of government services, the Government of Rwanda (GoR) recognized the need for a standardized approach to software security and privacy. This guideline consolidates the principles of Privacy by Design (PbD) and Security by Design, aligning with Law No 058/2021 on Data Protection and national minimum cybersecurity standards. It was developed to promote proactive, consistent, and auditable practices across all government software projects.

Objectives

This guideline aims to provide clear, actionable instructions to embed security and privacy into software systems used by the Government of Rwanda. It seeks to:

- Ensure confidentiality, integrity, availability, and privacy of personal data throughout the software lifecycle.
- Provide standardized, auditable steps and deliverables for all phases of software development, deployment, and maintenance.
- Promote proactive identification and mitigation of security and privacy risks.
- Align software practices with Law No 058/2021 (Data Protection) and national cybersecurity standards.
- Support a consistent approach across GoR institutions, contractors, and service providers.

Intended outcomes

Following this guideline, users should be able to:

- Implement secure and privacy-aware software systems from initiation to decommission.
- Minimize risks of data breaches or unauthorized access.
- Maintain compliance with legal and regulatory requirements.
- Enhance public trust in digital government services.

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.

Target Audience Roles and Responsibilities

Key roles include:

- **Management:** Approve security and privacy deliverables and ensure resourcing.
- **System owners:** Classify data, approve risk treatment, and ensure compliance.
- **Project managers:** Include security tasks in plans and enforce deliverables.
- **Security expert:** Lead threat/risk assessments, reviews, and testing.
- **Developers:** Implement secure code and remediate findings.
- **System administrator:** Apply configurations, patching, and continuous monitoring.
- **Database administrators:** Secure, manage, and monitor databases to protect and maintain data.

List of Abbreviations

- **RISA:** Rwanda Information Society Authority
- **GoR:** Government of Rwanda
- **PbD:** Privacy by Design
- **BYOD:** Bring Your Own Device
- **RBAC:** Role-Based Access Control
- **PAM:** Privileged Access Management
- **MFA:** Multi-Factor Authentication
- **OWASP:** Open Worldwide Application Security Project
- **CERT:** Computer Emergency Response Team
- **CIA:** Confidentiality, Integrity and Availability
- **PIA:** Privacy Impact Assessment
- **SAST:** Static Application Security Testing
- **CI/CD:** Continuous Integration / Continuous Deployment
- **DAST:** Dynamic Application Security Testing
- **IDS/IPS:** Intrusion Detection System / Intrusion Prevention System
- **SIEM:** Security Information and Event Management
- **KPIs:** Key Performance Indicators
- **NCSA:** National Cyber Security Authority

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.

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.

Software development lifecycle step-by-step guidance

Below are phase-by-phase actions, mandatory deliverables and practical checklists to guide implementation.

Software development lifecycle step-by-step guidance

Initiation

Goal: Establish security and privacy expectations and identify risks before design work begins.

Actions:

1. Appoint project sponsor, system owner and security lead.
2. Perform initial Threat and Privacy Risk Assessment (documented).
3. Define security and privacy objectives of CIA, non-repudiation and legal requirements.
4. Draft a Security and Privacy Plan with milestones, roles and budget for security activities.
5. Require security awareness briefing for project stakeholders.

Software development lifecycle step-by-step guidance

Requirements and acquisition

Goal: Ensure requirements include explicit privacy and security criteria.

1. Define functional, privacy and security requirements. Include purpose limitation and data minimization requirements.
2. Conduct Privacy Impact Assessment (PIA) and update risk register.
3. Translate risks into measurable security requirements like encryption, RBAC, logging and retention.
4. For procurement: include security clauses, acceptance criteria and tender security evaluation.
5. For third parties: require evidence of prior security audits and contractual data protection obligations.

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.

Software development lifecycle step-by-step guidance

Development

Goal: Implement secure, privacy-aware code and configurations.

1. Adopt secure coding standards (OWASP, CERT) and include them in the definition of done.
2. Use automated static analysis (SAST), dependency scanning and secret detection in CI/CD pipelines.
3. Enforce strong access controls for development environments and use separate secrets management.
4. Perform regular code reviews focused on security and privacy by identifying hard-coded secrets and data exposures.
5. Implement privacy-enhancing techniques (pseudonymization, tokenization) where feasible.
6. Maintain secure build and deployment scripts; avoid embedding credentials in code.

Testing

Goal: Verify security and privacy controls work as intended.

1. Create a security test plan covering unit, integration, system, and acceptance tests.
2. Include privacy test cases validating consent, data minimization, and access controls.
3. Conduct vulnerability scanning and dynamic application security testing (DAST).
4. Arrange independent penetration testing for critical systems and production environments.
5. Perform usability testing to ensure privacy settings and notices are clear and actionable.
6. Run regression tests after patches and new features to prevent reintroducing vulnerabilities.

Software development lifecycle step-by-step guidance

Deployment

Goal: Deploy securely with correct configurations, access controls and monitoring in place.

1. Apply secure configuration baselines and hardening to servers, databases and network devices.
2. Enforce RBAC and configure least privilege for all accounts; set up MFA for admin accounts.
3. Enable and protect audit logging; ensure log storage and retention meet policy requirements.
4. Conduct a production penetration test and address critical findings before go-live.
5. Publish privacy notices and provide user controls for consent and data management.
6. Establish monitoring and alerting (IDS/IPS, SIEM) and define on-call incident responders.

Operations and Maintenance

Goal: Sustain security and privacy posture throughout operations.

1. Maintain a schedule for vulnerability scanning, patch management, and configuration reviews.
2. Conduct periodic privacy and security control reviews and update PIAs as needed.
3. Ensure change management enforces security reviews and testing before changes are applied.
4. Continue training for administrators and users; run phishing and awareness programs.
5. Keep data retention schedules and securely sanitize or delete data when no longer required.
6. Keep an incident response plan current and conduct tabletop exercises regularly.

Upgrade / Decommission

Goal: Safely retire or replace systems while preserving required records and preventing data leakage.

1. Plan archival or migration of records according to legal retention requirements.
2. Sanitize media and verify secure deletion of sensitive data using approved methods.
3. Revoke access, disable accounts and remove credentials tied to decommissioned systems.
4. Update documentation to reflect where data was moved and how it can be accessed or destroyed.
5. Notify stakeholders and offer users guidance to export or delete their data where applicable.

Security Incident Management

Key steps:

1. **Prepare:** maintain an incident response plan with roles, communication trees, and escalation criteria.
2. **Detect and report:** ensure monitoring, logging and clear internal reporting channels.
3. **Classify:** use severity levels (critical, major, minor) and assign appropriate response teams.
4. **Contain and eradicate:** isolate affected systems and remove root causes.
5. **Recover:** restore services from trusted backups and validate integrity.
6. **Post-incident:** perform root-cause analysis, update risk registers, and publish lessons learned.

Awareness, Training and Best Practices

Provide role-specific training and general awareness sessions.

Topics should include:

- Data protection law and privacy (Law No 058/2021).
- Secure development lifecycle and secure configuration.
- Phishing awareness and safe handling of sensitive data.
- Incident reporting procedures and personal responsibilities.

Compliance, Audit and Continuous Improvement

Schedule regular audits, internal and external assessments, and maintain documented evidence for compliance. Update controls and PIAs when legal/regulatory or threat landscapes change. Use KPIs (e.g: time-to-patch, vulnerabilities found vs remediated) to drive improvements.

References

- Law No 058/2021 Relating to the Protection of Personal Data and Privacy.
- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, CISA, October 2023.
- Minimum Cybersecurity Standards for Public Institutions, NCSA, July 2023.
- https://privacy-by-design.ca/