Software Usage and Access Guidelines

This document provides guidelines on the appropriate and legal use of software and how access to software should be managed. The guidelines are designed to provide clear parameters for the responsible utilization of software resources within governmental institutions.

- Introduction
- Scope and Objectives
  - Security
  - Data Protection and Privacy
  - Preventing unauthorized modifications
  - Maintaining accountability
  - Resource management
  - Protecting Intellectual Property
- Procedures, Steps and Standards
  - Guidelines on Acceptable Software Use
  - Guidelines on User Access Management
- Monitoring and Compliance
- Review and Update
- Resources and Reference

Introduction

Government software plays a pivotal role in facilitating efficient operations and serving the public interest. Government software should be used responsibly and ethically to ensure integrity of software systems, safeguard sensitive data and uphold the public trust.

This document provides guidelines on the appropriate and legal use of software and how access to software should be managed. The guidelines are designed to provide clear parameters for the responsible utilization of software resources within governmental institutions.

Scope and Objectives

These software usage and access guidelines are applicable to all users of software solutions in Government of Rwanda institutions as well as the IT teams that implement and maintain them. They aim to maintain a consistent, secure and compliant computing environment, as well as to protect the organization and its staff from potential legal risks and liabilities. Key objectives of ensuring appropriate software usage and access include:

Security

Government software often handles sensitive information, including personal data of citizens, classified documents, and critical infrastructure data. Controlling access helps mitigate the risk of unauthorized access, data breaches, and cyberattacks that could compromise national security or public safety.

Data Protection and Privacy

Government software may contain confidential or personally identifiable information (PII) that must be protected according to privacy regulations. By controlling access, government agencies can ensure that only authorized personnel with a legitimate need to access this information can do so, reducing the risk of data misuse or exposure.

Preventing unauthorized modifications

Government software systems may include critical functions and processes that, if tampered with or modified by unauthorized users, could disrupt operations or compromise the integrity of government services. By controlling access, agencies can prevent unauthorized modifications and maintain the reliability and trustworthiness of their software systems.

Maintaining accountability

Controlling access to government software helps establish accountability for actions taken within the system. By assigning specific user accounts and permissions, agencies can track and audit user activity, making it easier to identify individuals responsible for any unauthorized actions or security incidents.

Resource management

Government software resources, including licenses, computing resources, and data storage, are often limited and must be allocated efficiently. Controlling access helps ensure that resources are used effectively by restricting access to only those who truly need it for their job responsibilities.

Protecting Intellectual Property

Government software may contain proprietary algorithms, code, or technologies developed for specific government purposes. Some of the software may also be licensed with specific restrictions that should be complied with. Controlling access helps protect these intellectual property assets from theft or misuse by unauthorized individuals or entities.

Procedures, Steps and Standards

Guidelines on Acceptable Software Use

Government institutions must ensure that all software is used in a lawful, ethical, and secure manner. This section outlines detailed procedures, Do's, Don'ts, and best practices for software usage within public institutions.

Intended Purpose [Mandatory]

Procedures:

- Users must use software applications strictly for their intended work-related purposes.
- Department heads should clearly define acceptable and unacceptable software uses within their units.
- IT departments should monitor software logs to detect non-compliant or unauthorized use.
- Any misuse should be reported immediately to the system administrator or designated ICT officer.

Do's	Don'ts	Best practice
Do use government software only for tasks that align with official duties.	Don't use government software for personal, commercial, or political activities.	Provide annual refresher training on acceptable software use.
Do follow approved workflows and security policies when using applications.	Don't upload, store, or process non-official data using government software.	Enforce disciplinary actions for repeated misuse or policy violation.
		Implement user activity monitoring tools for accountability.

Licensed Software [Mandatory]

Procedures:

- Only install software that has been properly procured and licensed by the institution.
- Maintain an up-to-date software inventory with license information and expiry dates.
- Periodically verify software compliance through license audits.
- Renew licenses before expiry and uninstall any unlicensed software immediately.

Do's	Don'ts	Best practice
Do read and understand software license agreements before installation.	Don't install pirated or unapproved software.	Schedule quarterly internal audits to check compliance with licensing policies.
Do store purchase and license documentation securely.	Don't share or copy software installers without authorization.	Engage RISA or the national procurement authority for enterprise-wide licenses when possible.

Intellectual Property [Mandatory]

Procedures:

- Verify ownership or licensing terms before using any third-party or open-source software.

- Acknowledge the developers' IP when modifying or integrating external code into government projects.
- Ensure that any customization of proprietary software follows contractual agreements.
- Report suspected IP violations immediately to the ICT management or legal department.

Do's	Don'ts	Best practice
Do respect copyright and patent laws.	Don't reverse-engineer, copy, or distribute proprietary software.	Establish an IP compliance checklist before system deployment.
Do use open-source software under approved licenses (e.g: Apache).	Don't use cracked or unauthorized versions.	Train IT staff and end-users on recognizing and respecting software IP rights.

Software Updates [Mandatory]

Step-by-Step Procedures:

- The IT department must develop a software update schedule for all critical applications.
- Enable automatic updates for operating systems, antivirus, and productivity tools when feasible.
- For non-automatic systems, conduct monthly patch management sessions.
- Document all updates performed for accountability and auditing.

Do's	Don'ts	Best practice
Do apply critical security patches as soon as they are released.	Don't postpone or ignore update notifications.	Test major updates in a controlled environment before deployment to production.
Do inform users before major updates that may affect system availability.	Don't install updates from untrusted or unofficial sources.	Maintain rollback plans in case updates cause service disruptions.

Reporting Violations [Recommended]

Procedures:

- Create an internal reporting channel using email, hotline or ticket system for users to report violations.
- Assign an ICT security focal point to receive, log, and act upon reported issues.
- Protect whistleblowers from retaliation and ensure confidentiality.
- Document all incidents, responses, and resolutions.

Do's	Don'ts	Best practice
Do encourage staff to report suspicious activities promptly.	Don't ignore minor incidents; report all issues for review.	Integrate violation tracking into the institution's Service Desk system.
Do include violation reporting in cybersecurity awareness sessions.	Don't share violation reports outside official channels.	Conduct post-incident reviews to identify root causes and preventive measures.

Storage Locations [Mandatory]

Procedures:

- Store all government software and data only on officially approved servers, data centers, or cloud platforms.
- Prohibit saving government data on personal USB drives, laptops, or unauthorized devices.
- IT teams must regularly back up software configurations and critical data.

- Apply encryption to data in storage and during transfer.

Do’s	Don’ts	Best practice
Do use secure government-managed repositories for storing software.	Don’t upload software or government data to public storage (e.g: Google Drive, Dropbox) unless officially approved.	Implement a centralized storage policy defining approved locations.
Do perform scheduled backups and verify data integrity.	Don’t use personal email to transmit installation files or system credentials.	Classify data according to sensitivity levels (public, confidential, restricted).
		Periodically review access permissions to storage systems.

Security Awareness [Mandatory]

Procedures:

- Conduct regular security awareness training for all employees and contractors.
- Include modules on phishing, malware prevention, and responsible software use.
- Display reminders on login screens or dashboards about secure usage practices.
- Evaluate user understanding through short quizzes or e-learning modules.

Do’s	Don’ts	Best practice
Do stay alert for phishing emails or suspicious links.	Don’t open attachments from unknown senders.	Incorporate software security awareness into onboarding sessions.
Do immediately report any suspected malware or data breach.	Don’t install browser extensions or apps without IT approval.	Reward compliance and positive reporting behavior.
		Run simulated phishing tests quarterly to reinforce awareness.

Central Management [Recommended]

Procedures:

- All software installations must be performed or approved by the central IT unit.
- Use centralized management tools to deploy and update software across all workstations.
- Regularly synchronize software inventory to detect unauthorized applications.
- Establish an institutional software catalogue of approved and supported applications.

Do’s	Don’ts	Best practice
Do manage all installations from central repositories or IT-managed servers.	Don’t allow staff to install or modify software independently.	Adopt an endpoint management platform (e.g: Ansible).
Do enforce standard configurations for uniformity.	Don’t maintain outdated or redundant applications.	Schedule monthly compliance scans to ensure all systems meet software standards.
		Maintain centralized logs for auditing and troubleshooting.

Guidelines on User Access Management

User Access Management is the process of creating, managing, and securing user accounts on software systems. It ensures that only authorized personnel can access government systems, protects sensitive data, and maintains accountability. This section outlines the mandatory procedures, standards, and best practices that every government institution must follow to manage user access effectively.

Authorized Access [Mandatory]

Ensure that only legitimate, authorized users can access government software applications according to their job roles and responsibilities.

Step-by-Step Procedures:

- Define user roles and responsibilities before granting access.
- Submit an Access Request Form approved by the user's supervisor or department head.
- The IT administrator reviews the request for necessity, role alignment, and risk.
- Access is granted based on the principle of least privilege (users only get access needed to perform their duties).
- Maintain a user access register with details of all users, roles, and permissions.

Do's	Don'ts	Practice
Do verify each user's identity before granting access.	Don't grant administrative rights unless necessary.	Implement role-based access control (RBAC).
Do review access rights periodically (every 3–6 months).	Don't approve access requests without written authorization.	Automate access approval and logging through identity management tools.
		Require annual user access recertification.

Termination of User Accounts [Mandatory]

Prevent unauthorized access from former employees, contractors, or temporary users.

Procedures:

- HR or department heads must immediately notify the IT department when an employee resigns, transfers, or is terminated.
- IT staff must disable or delete the user account within 24 hours of notification.
- Remove associated access rights, including email, VPN, cloud services, and databases.
- Transfer or archive the user's data according to the institution's data retention policy.
- Conduct quarterly audits to detect dormant or unauthorized accounts.

Do's	Don'ts	Practice
Do confirm account termination with written acknowledgment from HR.	Don't leave inactive accounts enabled.	Use an automated deprovisioning system linked to HR exit workflows.
Do maintain a record of all deactivated accounts.	Don't reuse deleted usernames without clearance.	

Third-Party Access [Mandatory]

Ensure that external vendors or partners access government software systems securely and temporarily.

Procedures:

- Require third parties to sign a Confidentiality and Non-Disclosure Agreement (NDA).
- Access must be formally requested and approved for a specific purpose and time frame.
- Create a dedicated account for the third party with limited privileges and log all activities.
- Monitor sessions in real time, especially for production environments.
- Disable access immediately after task completion.

Do's	Don'ts	Practice
Do verify the identity and legitimacy of all third-party users.	Don't provide administrative credentials.	Use a secure remote access gateway or jump server for vendor sessions.
Do audit third-party access logs monthly.	Don't allow shared or unmonitored VPN connections.	

Generic or Shared User Accounts [Mandatory]

Maintain accountability by ensuring all actions on systems are traceable to an individual user.

Procedures:

- Prohibit creation of shared or generic accounts.
- All users must have unique credentials.
- If a shared account is unavoidable, document who used it, when, and for what purpose.
- Implement enhanced logging and multi-factor authentication (MFA) for such accounts.

Do's	Don'ts	Practice
Do maintain accountability records for exceptional shared access.	Don't use shared accounts for daily operations	Integrate systems with centralized directory services (e.g: Active Directory) to enforce identity traceability.

Securing Login Credentials [Mandatory]

Protect user credentials from unauthorized disclosure or misuse.

Procedures:

- Users must create strong passwords according to institutional policy.
- Never write passwords on paper or share them verbally or electronically.
- Change passwords immediately if a breach is suspected.
- IT teams should encrypt passwords in storage and transmission.

Do's	Don'ts	Practice
Do use password managers approved by the IT department.	Don't reuse passwords across systems.	Implement automatic password rotation for privileged accounts.
Do lock your screen when away from your workstation	Don't disclose login credentials via email or chat.	

Password Policies [Mandatory]

Ensure consistent and secure password management across all systems by following the Standards (based on NIST SP 800-63B):

- Minimum length: 8–12 characters.
- Must include uppercase, lowercase, numbers, and special characters.
- Password expiry: every 90 days (or use continuous monitoring if MFA is enforced).
- Lockout after three (3) failed attempts.

Procedures:

- IT administrators configure password policies in all systems.
- Users are informed during onboarding.
- Systems log password change history for auditing.

Do's	Don'ts	Practice
Do encourage use of passphrases.	Don't force frequent unnecessary password changes (unless a breach occurs).	Adopt adaptive authentication where risk-based password validation is applied.

Multi-Factor Authentication (MFA) [Mandatory]

Enhance security by requiring more than one factor of authentication.

Procedures:

- Implement MFA for all high-privilege accounts and sensitive applications.
- Combine at least two of the following:
- Something you know (password).
- Something you have (security token or code).
- Something you are (biometric trait).
- Provide users with setup guidance and recovery options.

Do's	Don'ts	Best practice
Do enforce MFA for VPN, email, and system admin logins.	Don't allow exceptions without written approval from IT Security.	Regularly review and update MFA settings to ensure only authorized users have active access.

Biometrics [Recommended]

Add an additional layer of user authentication to enhance security and convenience.

Procedures:

- Implement biometric authentication (fingerprint, face, or iris recognition) in systems supporting it.
- Ensure compliance with Rwanda's Data Protection and Privacy Law for biometric data handling.
- Provide alternative authentication for users who opt out of biometrics.
- Store biometric templates securely using encryption and hashing techniques.

Do’s	Don’ts	Practice
Do inform users about how their biometric data is used and stored.	Don’t use biometric data for non-authentication purposes.	Combine biometric authentication with MFA for sensitive or high-security systems.
Do restrict biometric data access to authorized security personnel only.		

Monitoring and Compliance

Compliance with this guideline shall be monitored by the institution’s ICT department in collaboration with RISA. Regular reviews, internal audits, and access log inspections must be performed to detect non-compliance or security violations. Failure to comply may lead to disciplinary action or legal consequences under GoR ICT regulations.

Review and Update

This document shall be reviewed every two years or sooner if technological or policy changes occur. The review process shall be led by RISA in consultation with government ICT managers.

Resources and Reference

- Rwanda Data Protection and Privacy Law (2021)
- National Cyber Security Policy
- NIST Digital Identity Guidelines (SP 800-63B)