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.

Revision #2
Created 14 October 2025 07:21:50 by RISA
Updated 14 October 2025 08:42:00 by RISA