Software applications

- **Architectural model for e-government applications:** all systems should be documented in five viewpoints including the enterprise viewpoint (describe purpose, scope and processes), the information viewpoint (determines the structure and semantics of the system's information), the computational viewpoint, the engineering viewpoint, and the technology viewpoint.
- **Software design:** any new software design should consider security by design, reusability, scalability, information sharing, user satisfaction, improved productivity, compatibility, interoperability, unified support, and cost-effectiveness, as principles.
- **Acquisition of new software:** competent team (EA team at institutional or sector level) has to be consulted in order to determine whether the new software is needed, and to assess if it is to be developed internally or externally.
- **Proprietary and open sources software:** should be treated equally depending on the advantages and benefits to the Government according to the defined software design principles and in regards to the needs and requirements at institution level.
- **Software development:** RISA should be consulted to approve development languages and platforms.
- **Software license:** only genuine licenses are allowed in government institutions. The choice of licensing mode (user-based or server-based) should take into account cost-effectiveness. The procurement of commonly procured licenses should be done through a centralized framework.
- **Software maintenance:** there should be a focal team at institution level, which should elaborate the maintenance plan to collaborate with RISA on regular basis for periodically system audits, maintenance, updates, vulnerabilities assessment, obsolescence of their systems, so to ensure maximum system availability.
- **Systems and software phase-out:** the phase-out or upgrade of any system or The application should be done in collaboration with RISA, and the security of information contained should be considered.
- **Messaging and collaboration:** the use of official emails should be enforced, and each institution should comply with the information security policy.
- **Antivirus:** Antivirus software should support a local license server and update server and provide automatic updates of the license server from the vendor site. Clients should get automatic updates from the local license server in case of non-availability of the update license server. The antivirus should support all available versions of the Microsoft Windows operating system (on the market) and should be browser/version independent. The network deployment feature should include virus updates status, license usage, client status, and installed machines.
- **Websites:** the web should be designed according to official template for government institutions; should be hosted at the national data center; web content should be update timely, and the website should be monitored.

Revision #1
Created 1 October 2025 10:40:43 by RISA
Updated 1 October 2025 10:44:53 by RISA