Software Applications and Data

- Software applications
- Data

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.

Data

- **Data availability:** Data should be available round the clock (24-hour access) to access from different time zones.
- **Data creation:** single point of capture, duplication of data capture should be avoided as much as possible.
- **Standardization of shared data:** should comply with any interoperability framework defined at institutional or sector level.
- **Data identifiers:** each shared data object should be identifiable by a globally unique identifier.

  Data backup and recovery: every institution should have in place a backup and recovery strategy; all data should be available both onsite and offsite.

  GoR's entities are required to host all IT systems and applications, which process, store and provide critical Government data and information in the National Data Center (NDC). These include core business applications and databases, emails systems, and websites.
- **Categories of data to be protected:** application and databases, email systems websites, operating systems, data on personal computers in institutions:

  − For critical IT systems and applications hosted in NDC, the institution should ensure that they subscribe to a minimum hosting plan that includes daily backups and disaster recovery services.

  − For critical IT systems and applications hosted on premises, the government entity should immediately consult RISA to devise a strategic road map for migration to the National Data Center.

  − Pending full migration of critical IT systems and applications to NDC, Government institutions are required to comply with the detailed data backup schedule as
  section I.

  − For other IT systems and applications deemed non-critical and kept on premises, entities are required to comply with detailed backup schedule.

  − For government data that resides on personal computers (Laptops & Desktops),
  government institutions are required to set up a local file server that automatically synchronize with users' personal computers to keep copies of any data files as created/updated by users.

  − Personal computers should also be installed with an up-to-date
  Antivirus/Antimalware and no user should be allowed to keep government data on a non-protected personal computer.

  − Personal computers and servers installed with Windows Operating Systems
  should be upgraded to Windows 10 (for desktops and laptops) and to at least Windows Server 2008 (For servers). In the meantime, IT teams should ensure that there is no single machine still running Windows XP in any institution, and that all Windows 7, 8 are up to date with the latest updates/patches.