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.

Revision #1
Created 1 October 2025 10:45:59 by RISA
Updated 1 October 2025 10:49:29 by RISA