Software Applications and Data

This section provides high level guidelines for software applications development, acquiring, usage and their security. It also provides guidelines for data processing, usage and protection.

- Software applications
- Data
- Business Continuity (BC) and Disaster Recovery (DR)

Software applications

- **Architectural model for e-government applications:** All systems shall be documented in five viewpoints including the enterprise viewpoint (describing purpose, scope and processes), the information viewpoint (determining the structure and semantics of the system's information), the computation viewpoint, the engineering viewpoint and the technology viewpoint.
- **Software design:** Any new software design shall consider security by design, privacy by design, reusability, scalability, information sharing, user satisfaction, improved productivity, compatibility, interoperability, unified support, and cost-effectiveness, as principles. Each Government institution shall have comprehensive and detailed requirements and design documents for each software solution they manage.
- **Acquisition of new software or upgrade:** The digitalization office in collaboration with RISA shall determine whether the new software or upgrade is needed, and once justified, assess if it is to be developed internally or externally.
- The digitalization office can internally develop and implement the solution if they have the required resources, competencies and skills. In case the digitalization office cannot develop the solution internally, they shall utilize the RISA framework contract. In case the solution cannot be implemented under the framework contract, the institution shall officially request a non-objection from RISA to utilize other alternative options.
- Institutions should follow the ICT Spend Control Guidelines for Public institutions when acquiring new software.
- **Proprietary and open-source software:** Proprietary and open-source software shall be treated equally depending on the advantages and benefits to the institution according to the defined software design principles and regarding the needs and requirements at institution level. The institution with such a solution shall have the required training for its staff in order to have skills to maintain and support it.
- **Security Patch Management:** The institution managing the application/systems or a third party on behalf of the institution shall make sure that security patch management is done regularly and prioritize critical patches to address vulnerabilities promptly. The software source code for proprietary software shall reside in a centralized version control platform recommended by RISA.
- **Software development methodology:** Software solutions shall be developed following agile methodology and the development team shall focus on customer satisfaction, quick software delivery and response to change.
- **Software license:** Only genuine licenses are allowed in government institutions. The procurement of commonly procured licenses shall be done through a centralized framework. In case the licenses cannot be acquired under the centralized framework, the institution shall officially request for a non-objection from RISA. The choice of licensing mode (user based or server based) shall consider cost efficiency.
- **Software maintenance:** there shall be a focal team at institution level which shall elaborate the maintenance plan and collaborate with RISA on regular basis for periodic system audits, maintenance, updates, vulnerabilities assessment, and obsolescence of their systems, so as to ensure maximum system availability. A vulnerability assessment

plan shall be made available by the digitalization office for each institution and make sure that all systems are secured with updated antivirus software.

- **Systems and software phase out:** the phase out of any system or application shall be done in collaboration with RISA and the security of information contained in the system shall be considered. The phase out shall be based on each institutions criteria for the required phase out especially after a phase out assessment has been done, and related reports shall be availed for effective decision making.
- **Websites:** Websites of government Institutions shall be designed according to the official template provided by RISA. These websites shall be hosted at the National Data Center. Web Content shall be updated timely, and the website shall be monitored by the Institution. All websites of government institutions should be registered under the .gov.rw subdomain while those in the academic sector should be under .ac.rw. The requests for the .gov.rw domain should go through RISA before submission to the competent issuing institution for approval.

Data

Data produced or collected by government institutions is necessary for measuring effectiveness and developing public services. In that sense, institutions are expected to perform the following:

- Data discovery and metadata capture.
- Search and filtering.
- Business Glossary.
- Data Quality Monitoring.

This shall allow public institutions to reduce the time it takes to find the right data and to facilitate more data-informed decisions. Data shall also be classified by access level, specifying which data is accessible to the public, government institutions, Private and other partners.

- The value in data sharing between government institutions lies in the ability to use the data for meaningful insights. For guidelines on data sharing, refer to the data sharing policy.
- Categories of data to be protected shall include but not limited to applications and databases, email, websites, operating systems, data on personal computers among other data. Encrypt sensitive data both in transit and at rest, using strong encryption algorithms and ensure that encryption keys are securely managed and stored.
- All government data shall be hosted locally at the institution or within Rwanda and the institution owning it shall determine who to share the data with based on access levels. Depending on the type of data, the duration of retention shall be determined by the institution owning the data.
- Data and data storage breaches shall be avoided, and security safeguards shall be put in place by the institution holding the data. For effectiveness, personal and sensitive data shall be classified to cater for security and use by putting into consideration measures to conduct and have data backups to prevent data loss by all government institutions.
- All institutions shall also be obliged to enforce the requirements of the Data Protection and Privacy Law Nº 058/2021 of 13/10/2021.
- The Data Protection Law shall be used as a guide to determine the processing of Personal data and sensitive data, and all institutions shall be obliged to comply with this law. Under this law,
- processing of data is an operation or set of operations which shall be performed on personal data or on sets of personal data and sensitive data whether or not by automated means, such as access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction.
- The Data protection and Privacy law also provides safeguards to process sensitive and personal data. In other words, security of processing this involves the ability to ensure confidentiality, integrity and availability of data. It is recommended to all public institutions to perform a Data Protection Impact Assessment (DPIA).

- Data protection impact assessment helps to assess the impact of a process or project more specifically a processing that an institution is going to carry out. DPIA aimed at two important understandings; the understanding of the risks to individuals (data) as well as the understanding if the processing is necessary and proportionate and most importantly identifying security measures in place or needed and their adequacy level.

Business Continuity (BC) and Disaster Recovery (DR)

Business continuity management is a planning and holistic management through which institutions create and implement measures, strategies and plans which are effective to manage crises, respond to/ and recover from a disaster.

Business continuity is more than just a plan to recover from a disaster but a survival strategy for enterprises that enhances systems resilience, ensures high availability and continuous operations of solutions. All institutions shall therefore have Disaster Recovery plans as a measure and guide to use for Business Continuity in case disasters befall.

Disaster recovery consists of developing step-by-step procedures for ensuring a full recovery, however, when many think about DR, they usually think about Backup, while it is only one piece in BC-DR. Therefore, the following are recommended to be followed for best practices:

A. Based on the data and systems inventory and classification:

- All institutions shall have a backup mechanism for all data that is performed regularly and most importantly kept offsite; this means having taken your backups, stored them in a safe and accessible way. Local Backup on Recovery Devices shall be stored in house and then replicated
- to an offsite location where applicable. It is the local site that shall serve a master role and then the offsite backup.
- For important data and systems, all institutions shall have a Hot-standby DR solution based on both the Business Continuity and Disaster Recovery plans.
- For critical data and systems having a DR solution shall no longer be an option but an active-active DR solution by which both primary and secondary sites shall be active and processing requests in parallel. This solution shall not help in recovery and continuity of the business after the disaster but shall avoid a disaster altogether by minimizing the risk of losing data, systems and information The Recovery time objective and Recovery point objective (RPO and RPO shall be near to zero).
- For further clarifications and understanding about Disaster recovery and Business continuity refer to the current Business Continuity Management guidelines issued by RISA.
- For critical IT systems and applications hosted in the National Data Centre, the institution shall 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 shall 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 the National Data Centre and other IT systems and applications deemed non-critical and kept on premises, Government institutions shall be required to comply with the institution’s detailed data

backup schedule.

- For government data that resides on personal computers (Laptops & Desktops), government institutions shall set up a local file server that automatically synchronizes with users' personal computers to keep copies of any data files as created/updated by users.
- Personal computers shall also be installed with an up-to-date Antivirus/Antimalware and no user shall be allowed to keep government data on a non-protected personal computer.
- Personal computers and servers shall have the latest Operating Systems installed or upgraded to the latest operating system.