

Scope and Objectives

These software usage and access guidelines are applicable to all users of software solutions in Government of Rwanda institutions as well as the IT teams that implement and maintain them. They aim to maintain a consistent, secure and compliant computing environment, as well as to protect the organization and its staff from potential legal risks and liabilities. Key objectives of ensuring appropriate software usage and access include:

- Security
- Data Protection and Privacy
- Preventing unauthorized modifications
- Maintaining accountability
- Resource management
- Protecting Intellectual Property

Security

Government software often handles sensitive information, including personal data of citizens, classified documents, and critical infrastructure data. Controlling access helps mitigate the risk of unauthorized access, data breaches, and cyberattacks that could compromise national security or public safety.

Data Protection and Privacy

Government software may contain confidential or personally identifiable information (PII) that must be protected according to privacy regulations. By controlling access, government agencies can ensure that only authorized personnel with a legitimate need to access this information can do so, reducing the risk of data misuse or exposure.

Preventing unauthorized modifications

Government software systems may include critical functions and processes that, if tampered with or modified by unauthorized users, could disrupt operations or compromise the integrity of government services. By controlling access, agencies can prevent unauthorized modifications and maintain the reliability and trustworthiness of their software systems.

Maintaining accountability

Controlling access to government software helps establish accountability for actions taken within the system. By assigning specific user accounts and permissions, agencies can track and audit user activity, making it easier to identify individuals responsible for any unauthorized actions or security incidents.

Resource management

Government software resources, including licenses, computing resources, and data storage, are often limited and must be allocated efficiently. Controlling access helps ensure that resources are used effectively by restricting access to only those who truly need it for their job responsibilities.

Protecting Intellectual Property

Government software may contain proprietary algorithms, code, or technologies developed for specific government purposes. Some of the software may also be licensed with specific restrictions that should be complied with. Controlling access helps protect these intellectual property assets from theft or misuse by unauthorized individuals or entities.