### 2.2 - Non-Functional requirements

The non-functional requirements are divided into five categories based on their influence on our program, including **Efficiency requirement, Usability requirement, security requirement, scalability requirement,** and **ethical requirement.**

**NFR1 Efficiency requirements**

Efficiency requirements specify and constrain the storage space limitation and processing time of the software.

|  |  |
| --- | --- |
| Type | NFR1.1 Storage space limitation |
| Metrics | Monitor and manage storage space consumption to stay within defined limits of 10GB. |
| Security | Restrict access to limited roles to ensure data security. |
| Constraints | Ensure data storage and access control align with data privacy regulations and security standards. |

|  |  |
| --- | --- |
| Type | NFR1.2 Processing time |
| Metrics | Measure the system's response time for various operations and monitor the delay or waiting time experienced during processing in the 20s. |
| Security | Use encryption for data at rest and in transit to protect sensitive information during processing |
| Constraints | Ensure that the processing time aligns with the available hardware resources and doesn't exceed system capabilities. |

**NFR2 Usability requirements**

Usability requirements specify and constrain the utility, flexibility, and robustness of the software.

|  |  |
| --- | --- |
| Type | NFR2.1 Utility and convenience |
| Metrics | The user can use it even if they don’t have IT skills |
| Security | None |
| Constraints | Users should find the navigator and other instructions simply accessible. |

|  |  |
| --- | --- |
| Type | NFR 2.2 Flexibility |
| Metrics | The user can use the software under OS and Windows |
| Security | The login process should be protected by the third-party verified software, for example, Microsoft Authenticator. |
| Constraints | It should be used to test and identify the user's operating system and to set all of the software to the appropriate level. |

|  |  |
| --- | --- |
| Type | NFR 2.3 Robustness |
| Metrics | The system follows ACID (Atomicity, Consistency, Isolation, Durability) properties. This ensures that data changes are not lost, and transactions are handled reliably. |
| Security | None |
| Constraints | Using a method or mechanism to catch errors related to data. |

**NFR3 Security requirements**

Security requirements specify and constrain data security and account security.

|  |  |
| --- | --- |
| Type | NFR 3.1 Data security |
| Metrics | Any third party should not be able to view private user data and not be able to access it. |
| Security | Ensure that only authorised personnel have access to the systems and tools used for data security. Implement access control policies and regularly review and update user permissions. |
| Constraints | Using third-party services or organisations are constrained by the security practices and measures of those third parties. |

|  |  |
| --- | --- |
| Type | NFR 3.2 Sign-in security |
| Metrics | Plug-in functions and software should protect the sign-in process. |
| Security | None |
| Constraints | limitation of password entering time, Confirmation through email when logging in |

**NFR4 Scalability requirements**

Scalability requirements specify and constrain support for large data.

|  |  |
| --- | --- |
| Type | NFR 4.1 supports large data |
| Metrics | The system is capable of potentially handling higher volumes, whether it be a greater number of users, increased throughput, or larger datasets. |
| Security | Managing and securing large datasets can be particularly challenging, as there may be increased risks associated with data breaches, data loss, and other security vulnerabilities. |
| Constraints | Ensuring that the system can scale seamlessly as data volumes grow is a constraint that requires careful planning and infrastructure design. |

**NFR5 Ethical requirements**

Ethical requirements specify and constrain data protection.

|  |  |
| --- | --- |
| Type | NFR 5.1 Data protection |
| Metrics | Collect the data with consent |
| Security | Only users holding the role “Customer advisor” or “Supervisor” can update the customer record |
| Constraints | Organisations must comply with various data protection laws and regulations |