**S16540**

**Non - Functional Requirements**

1. Safety Requirement

The framework is secured because it will give access to approved users. It’ll have a legitimate login framework which is able to require client id and password. The database is secured from SQL Injection methods with the assistance of private keys and a SSL/TLS key encryption. This guarantees that all information passed between the internet server and browsers stay private and indispensable.

1. Security Requirement

It is more secure than the current websites because it is not only ensured by the encryption of institute’s servers but also by SSL/TLS encryption which can halt SQL Infusion endeavors. The database cannot be modified by the client and as it can only be done by the system’s data administrator of the website. The key web administrations security necessities are confirmation, authorization, information security. In the proposed site verification is required for getting to information through legitimate channels. Security system typically grants access to accounts when users enter the correct username and strong password. A strong password should contain a certain number of characters, a capital letter and a symbol. After a certain number of login attempts, a security system may lock an account to protect a user’s information from potential hackers. To unlock their account, a user can contact the administrator to verify their identity and set a new password. It is only after the authentication that they can access the information on the website. Data is ensured employing a private key which uses SSL encryption. All system data must be backed up every 24 hours and the backup copies stored in a secure location which is not in the same building as the system. All external communications between the system’s data server and clients must be encrypted.