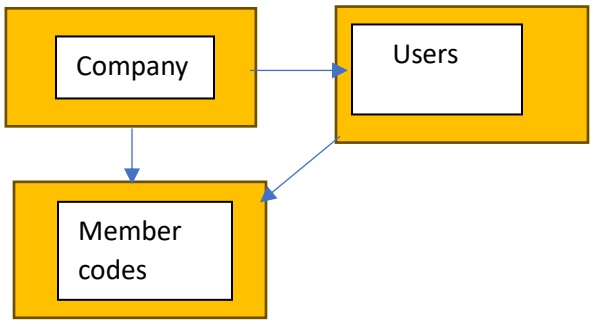
Security in NJUNS

NJUNS software is designed to ensure the data stored is only accessible to the parties allowed to access it. This is achieved in the following ways:

1. Hierarchy controls



The company is created in NJUNS. Users are assigned to their company. Companies can have multiple member codes. Users can only see tickets that involve their company or the member codes in their profile. Users can only edit the tickets involving the member codes in their profiles.

2. For the scenarios involving contractors, approval from the company they are contracting with is required before they are allowed access to NJUNS. Once approved, they will only see the tickets involved with the approved member codes in their profiles. The contracting company created in NJUNS does not have access to any tickets. NJUNS requires a Non-Disclosure Agreement (NDA) to be on file for all contracting companies.

3. NJUNS software utilizes Vaadin Server-Side Framework. The target web application utilizes Vaadin as a server-side framework, which provides several foundational security controls to establish a strong baseline security posture. First, Vaadin automates the communication between server and client through a single, secure endpoint. This greatly reduces the viable attack surface possible for an attacker to target. Additionally, as credentials are never transmitted to the client and processing ultimately occurs on the server, traditional password attacks are not feasible. Lastly, as Vaadin appears to be a security minded framework, built-in mitigations against serious vulnerabilities are in place such as cross-site scripting (XSS) and cross-site request forgery (CSRF).