eService Online Security Control Requirement

# Authentication

eService Online is an intranet web application, it is only accessible within Sanjel network. A valid domain user account is authenticated automatically through Windows Authentication.

User domain account name is used as user name in Sanjel Security Service.

Example: Adam has a valid Sanjel domain user account awang, he can access eService Online from a computer in Sanjel intranet logged in by using his domain account.

# Authorization

eService Online Authorization system must be aligned with best practices of ASP.NET Core Security.

Use eService Security Service database as backend to manage and store authorization rules.

eService Online frontend access control is based the role defined in Sanjel Security Service. Based on the rule definition, following access controls need to be implemented.

* Tab page accessibility control
* Data based pop-up menu items construction control to limit the access of certain functionalities
* Data form page level data CRUD control
* Read/Write control against real-time interaction such as drag and drop feature to prevent unauthorized data modification.

## Roles

#### Administrator

* Has access to all pages of eService Online
* Can see all menu items in pop-up menus
* Has write privilege on all data

#### Dispatchers

* Has access to Rig Board Page
* Can see all menu items in pop-up menus with in Rig Board Page
* Has write privilege on the data presented in Rig Board

#### Field Manager

* Has read-only access to Rig Board Page
* Does not have operational features on Rig Board Page
* Has read-only access to Upcoming Jobs Page