# Manual procedures required for:

## Security

The system stores confidential and sensitive data about employees, administrators and the business. Therefore, below are the safety procedures that will be implemented to prevent Web application attacks. This will ensure that none of the data is threatened at any point.

* All employees require a password to login into the system. They are assigned usernames and generated passwords at first. Once the administrator creates an account, an email is sent to the employee with the generated password. In case the employee’s email was missing, the person creating the account will be notified with the generated password.

Users are then prompted to change their passwords as soon as they login. Passwords must be 6 -8 alphanumeric characters and are going to be encrypted in the database.

* Application auto-logout if the system was left idle for 15 minutes. Reliable mechanisms will logout the users by popping up Time Out or Session Expired messages. This will prevent loss of data in case of a power outage, and will prevent unauthorized individuals from accessing the system through an idle computer.
* Setting specific permission sets for different workgroups. This will allow the administrator to configure the credentials for all employees and workgroups. Thus allowing flexibility as it provides the option of granting temporary credentials for particular employees at given times.

## Operation

The system mainly operates over an online application that allows Direct Manipulation through multiple interface screens. Those screens are to be accessed using different devices like mobiles and pc’s taking in consideration the system’s requirements.

The entire system is based on widgets and allowing the flexibility of adding plug-ins for future scalability.

## Backup and Restore

Application data (from the database) must be backed up on regular basis. Our system will provide ***automatic ongoing data backup*** for time consuming input procedures i.e. schedules***.*** Due to the system’s nature, providing ongoing data backup for all procedures will cost a lot more than the cost of an error for example, recreating a single account. Instead ***full and******incremental backups***are to be scheduled automatically by the system’s administrator. Users with the right permission set can perform ***manual full data*** backup. They can create restore points using the system's wizard. The wizard will walk them through the steps required to back up all their data. All backed up files could then be removed for off site storage using external storage devices. This will protect users against hardware failures or any other unforeseen problems. Ultimately users could simply refer to a restore point from an existing backup file. They are then walked through in a wizard to complete the procedure.

## Data Archival

Most of the old data is to be archived annually. This will include schedules, shifts, and employment records.

Other records like Notifications and e-mail messages are not to be archived due to their irrelevance to the system and thus they are to be deleted every 3 months.

Similarly to backup and restore, an administrator or an employee with the appropriate set of permissions must manually schedule to archive the data using the system’s wizard.