# Privileges granted

For any roles that require full access to the databases such as Administration will require “All” privileges assigned. For personnel who work with our customers privileges “select”, “insert” and “update” will need to be assigned, for managerial positions an additional privilege of “delete” should be assigned.

## Implications of privileges:

“All” privilege allows the user to modify everything within the database including creating and deleting tables, modifying rows. This is done with the SQL statement “GRANT ALL PRIVILEGES ON (database).\* TO (user)” for administrators that require the privilege across multiple databases the “ON (database).\*” is to be replaced with “ON \*.\*”. The privileges granted to ordinary staff members allows them to view, add and update the data in the specified database, the SQL statement “GRANT SELECT, INSERT, UPDATE ON (database).\* TO (user)” is to be used, for managers the statement will become “GRANT SELECT, INSERT, UPDATE, DELETE ON (database).\* TO (user)”.

Ways to minimise attacks:

To minimise the chances of attacks all passwords are to be hashed by SHA256 as default from MYSQL, this eliminates the possibility for someone to steal passwords as they will not be stored as plain text. Inputs from a web page must be parametrised and sanitized to reduce the risk of SQL injection attacks.