|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Apartment | X | X | X | X |  |
| Complex | x | x | x |  | Must not be able to delete entire db |
| Expense | x | x | x | x |  |
| Lease | x | x | x | x |  |
| Maintenance | x | x | x | x |  |
| Manager | x | x | x | x |  |
| Rent payment | x | x | x | x |  |
| Tenant | x | x | x | x |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Administrator | Select | Insert | Update | Delete | Constraints |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Owner | Select | Insert | Update | Delete | Constraints |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Apartment | x |  |  |  |  |
| Complex | x |  |  |  |  |
| Expense | x | x |  |  |  |
| Lease | x | x |  |  |  |
| Maintenance | x | x |  |  |  |
| Manager | x | x | x | x | For hiring / terminating purposes only |
| Rent payment | x | x |  |  |  |
| Tenant | x | x |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Manager | Select | Insert | Update | Delete | Constraints |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Apartment | x |  |  |  |  |
| Complex |  |  |  |  |  |
| Expense |  |  |  |  |  |
| Lease | x |  |  |  |  |
| Maintenance | x | x |  |  |  |
| Manager |  |  |  |  |  |
| Rent payment | x | x |  |  |  |
| Tenant | x | x |  |  | Only for adding new |
| Tenant | Select | Insert | Update | Delete | Constraints |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Apartment |  |  |  |  |  |
| Complex |  |  |  |  |  |
| Expense |  |  |  |  |  |
| Lease |  |  |  |  |  |
| Maintenance |  |  |  |  |  |
| Manager |  |  |  |  |  |
| Rent payment |  |  |  |  |  |
| Tenant |  | x |  |  | Only for adding updated contact info |

SECURITY PLAN

The access to sensitive data and permissions to make changes will be managed with secure authentication, assigned roles and safeguards to prevent damage or loss of critical business data.

AUTHENTICATION:

The system Administrator will have direct access to the database through an SQL server log in which may be accessed only in the office on the network.

The business owner(s) will also have access to the database on the network through a personalized log in. They will also have access to the online application with a personalized log in.

The apartment managers will have personalized log-ins assigned to them by the system administrator for the application online.

The Tenants will have a log in to the online application based on their personal lease information.

ASSIGNED ROLES:

Administrator:

The administrator will have the role with the most permissions on the actual database in order for them to make changes, full access to query and the ability to add and delete tables in order for the database to thrive. The administrator will not be able to delete the entire database.

Owner:

The owner role will allow some permissions for access to make changes in manager tables and have access to view all other tables, but only permission to insert data into expense, lease, maintenance, manager, rent payment and tenant tables.

Manager:

The manager role will give the manager permission to access set procedures for making changes and adding new data to the maintenance, rent payment and tenant tables. Their access to change or add new data will be limited to performing set procedures through their online app access. They will be able to view other tables and have queries they can perform to provide the information for quarterly reports.

Tenant:

The tenant role will give the tenant access to update their personal contact information in order to keep it up to date, they will not be able to view, access or make changes anywhere else.

THREAT ANALYSIS/ DISASTER MANAGEMENT PLAN

Most changes to the database for all users other than the administrator will be allowed only through rigid stored procedures in order to prevent accidental data corruption or intentional data corruption. The administrator will be given access to make manual changes through sql server, but not able to delete or remove the entire database.

Access to make queries will be limited mainly to stored procedural queries or views based on regular business procedures including information needed to fill out quarterly reports.

Log-ins will use certificates on top of standard authentication to prevent impersonation from unauthorized individuals or locations. All log-ins will be automatically terminated for managers who leave employment with Wild Wood Employment as their details are removed from their Manager ID.

Idle windows over 5 minutes will require re-authentication to prevent from nearby unauthorized personnel from accessing sensitive data.

A stored backup will be provided each 24 hours and stored for 48 hours in a separate secure location. An online backup will also be secured every 24 hours to serve as an extra security measure should there be a disaster that covers a larger geographic area. There will be several hard backup disks used in sequence to prevent the loss of data should their be any catastrophic hardware or software failures.