



Login (Admin and guest) = Both user and guest may need to log in to perform certain actions, although the permission may differ based on roles.

System can verify the password if the password is correct so the guest will be able to see the activities. If the password is not correct, it will show the error.

Logout (Admin and guest) = Logout allows users and guests to end their session securely, protecting the system from unauthorized access once the user is done. This ensures the system's integrity and security. System will be locked down once the admin and guest wish to.

Search Record (admin and guest) = They may need to search for records within the system.

Add Data = only admin have permission to add and edit new data to the system. This ensures that data can be updated as needed and responsible for updating or modifying the data in the system. This ensures the data remains relevant and accurate. Adding and editing access isn't available to guests to maintain, controlled and secure enviroment.

Delete (Admin) = Admin should have permission to delete data from the system, to remove obsolete information. Deletion must be restricted to admins to avoid accidental or malicious loss of important data by less privileged users.

Export/ import data (admin) = The ability to export or import data is essential for backup, data migration, or sharing purposes. Admins are typically responsible for managing the flow of data outside the system, so the function is restricted to their roles.

Lockdown = the lockdown use case is essential for situations where the system needs to restrict access to certain functionalities, typically for maintenance or security reasons. This action would likely be available only to Admins as they are responsible for the security and operational management of the system.