User Access Controls

Objectives:

- Establish a hierarchy of power that grants users different levels of power.
- Give Admin roles master control of the system.
- Give Vendor roles access over their vendor files and information.
- Give Developer roles access to edit web UI and UX files.

Background:

User Access Controls will add a layer of security to our webapp. Establishing a hierarchy of power allows certain users such as admins and developers to have certain powers over other users. This will allow high-level roles to manage system contents as well as enhance user experience by keeping back-end designs hidden for lower level users such as vendors and normal users.

Requirements:

- Give all roles network access.
- Give admin roles all available privileges.
- Give vendor roles access to edit vendor files and user files.
- Give normal user roles access to edit user files.
- Give developer roles access to edit UI and UX files.

Success: An efficient hierarchy will be set in place, that assigns the proper permissions to their respective roles.

Failure: An ineffective hierarchy will be set in place that will clutter and entangle the permissions and their roles.

4.25.1 Functional

Req#	Priority	Description	Rationale
General / Base Functionality			
FR-UAC-G-001	1	Admin roles have all privileges	Changes cannot be made to the system files if a role does not have access to edit system files and make updates/changes.
FR-UAC-G-002	1	Vendor roles can edit vendor files, edit their user files and access networks.	Vendors should be able to list product information as well as their products on out site.
FR-UAC-G-003	1	Developer roles can edit UI/UX files.	Developers have front end website access to be able to make changes to UI and implement or update easy functionality for the user.
FR-UAC-G-004	1	Basic roles can edit user files and access the network	Basic roles should have permission to access their user files and make basic changes to their accounts

Security Requirements			
FR-UAC-S-001	1	Basic role, vendor role and developer role users can not have access to edit System files.	Permissions should not be entangled across accounts, it should be clear which roles get which permissions.

User Access Controls Diagram

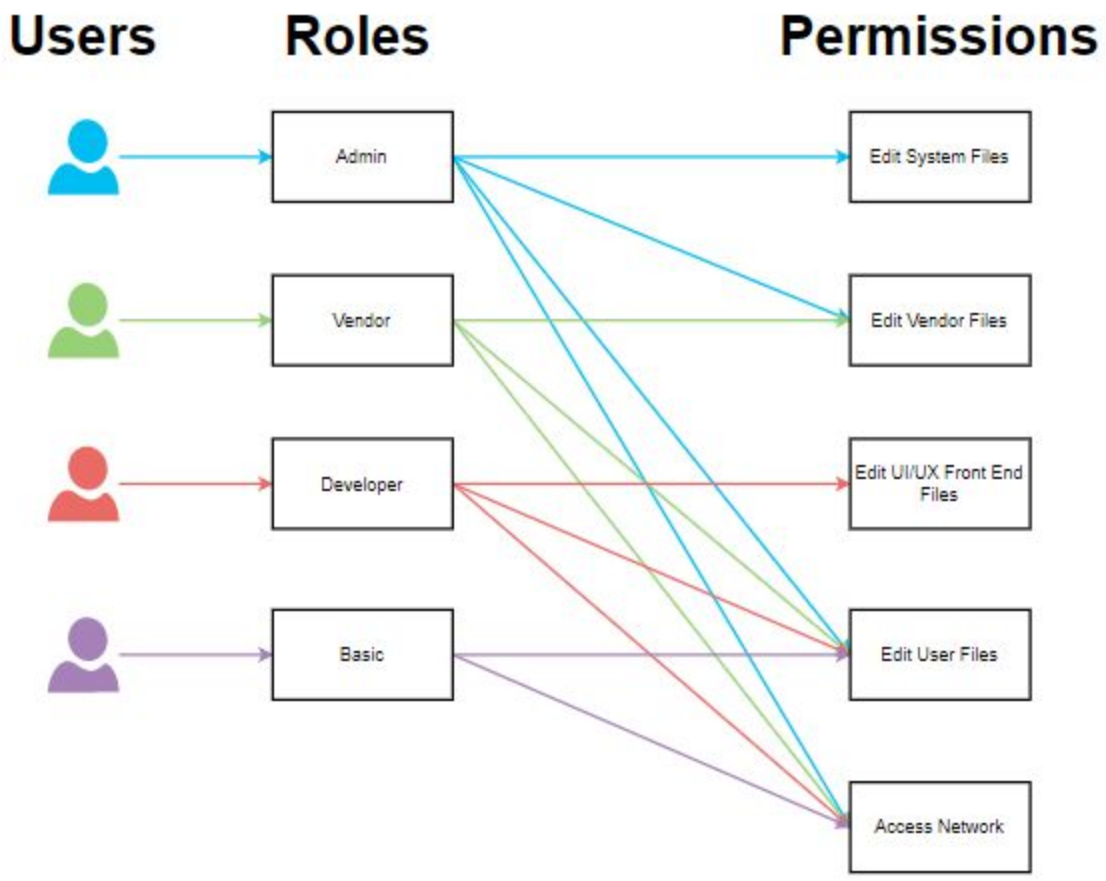

Fig.1 Role-Based Access Control