|  |  |  |
| --- | --- | --- |
| ***ID*** | ***Rule Definition*** | ***Source*** |
| BR-1 | Only users with a valid account can log in into the system | Authentication and security |
| BR-2 | Every user has their own unique account ID | Account database |
| BR-3 | Account’s password will be encrypted and can not be known by anyone but its user after completing the registration | Authentication and security |
| BR-4 | Restrictions on the format of the input information to avoid system errors | Authentication and security |
| BR-5 | User must login into system to be able to make transactions or edits | Authentication and security |
| BR-6 | Public users can view a peek of the information | Authentication and security |
| BR-7 | Admin can ban users out of the system if they have inappropriate behaviors | Account database |
| BR-8 | UI must be simple and easy to understand | UI |
| BR-9 | Error messages should be clear and easy to understand | UI |
| BR-10 | Content displayed must be honest and accurate | UI |
| BR-11 | Users have full discretion regarding their account information | Account Database |
| BR-12 | Admin can not cannot create false or fabricated information. | Database |
| BR-13 | Admin can not interfere into the log database | Security |
| BR-14 | User information will be protected and not provided or sold to outside parties. | Security |
| BR-15 | Admin can disable users for a period of time if they have inappropriate behaviors | Account database |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |