REQ-9: **Account Creation**

System Administrators must be able to create an account for another user. This account will start with no Access to the system, and a System Administrator must give them the level of access that the user requires.
Only System Administrators can create accounts.

REQ-10: **User Assignment to an Access Level**

System Administrators must be able to assign a user a new Access Level.

3.3 User Authentication

3.3.1 Description and Priority

- Users must first authenticate themselves with the Client System before using any of the functionalities provided.
- This also ensures users can only access the content they are meant to.

3.3.2 Stimulus/Response Sequences

- Every time a user wants to initialize a new session with the system, they will need to authenticate themselves.

3.3.3 Functional Requirements

REQ-11: **User Authentication**

Users trying to access the system must be authenticated in order to ensure they have the proper Access Level to interact with the system.
If a user cannot authenticate themselves, then they will have no access to the system.

REQ-12: **User Lockout**

Users who try to access the system, but fail to a given number of times, will become locked out of the system.
If any suspicious activity occurs, the User should be locked out of the system.
In order to reverse this, the User must speak with the System Administrator, who will reset the authentication details.

REQ-13: **User Authentication Reset**

A System Administrator can reset the authentication details of a user. If a user is no longer able to authenticate themselves, they should report to a System Administrator so this can be done.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The system may be processing very large amounts of data, so the maximum amount of time that the system should take to process a request is 24 hours.

System maintenance will occur at 11 PM EST/ 8 PM PST when required and will take a maximum of 2 hours to complete unless otherwise notified.

Since our system does not store any students' work on our processing server the client server must scrub the work of any identifying information. The scrubbing of information on a class size of 100 should take no more than 60 seconds. The minimum hardware requirements for the client system should be a dual core CPU with 4GB of RAM. The OS on the client system should be either Ubuntu 16.04 or newer, or any modern stable LTS unix flavour operating system.

The processing system should be able to receive at minimum five requests of sizes up to 5 GB simultaneously without faulting.

5.2 Safety Requirements

If the client system is set up incorrectly it is possible that students' work may be sent to an unknown server, to prevent any identity loss the data is stripped before it is sent. All data that is sent will be scrubbed of identifying information.

Normal computer safety precautions should be taken with the client system. For Example:

- Ensure the root password is sufficiently complex.
- Keep only necessary ports open.
- Keep security features up to date.

5.3 Security Requirements

All of the data that will be transmitted through the internet must be anonymised so no work can be identifiable if it is compromised during transmission.

The HTTP servers must use some sort of authentication such that any random person with the IP and Port can't send requests to the server. The requests should also be encrypted using HTTPS.

Every professor will have an account that will consist of a username and password, with the password being encrypted with bcrypt.