Functional Requirements

1.) ***Accuracy***—election systems should record the votes correctly

2.) *Verifiability and Auditability*—it should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records
    i. The system should allow voters to create a record of their vote that they can examine directly, and that can be used to audit equipment and elections.
    ii. The system must allow for recounts
    iii. All events and failures of the system should be recorded

3.) *Reliability*—election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of Internet communication.

4.) ***Flexibility***—election equipment should allow for a variety of ballot question formats (e.g., write-in candidates, survey questions, multiple languages); be compatible with a variety of standard platforms and technologies; and be accessible to people with disabilities.

5.) *Convenience*—voters should be able to cast votes quickly with minimal computer skills.
    i. The system should be as easy and straightforward as possible so as to minimize intimidation and confusion on the part of the voters

6.) *Certifiability*—election systems should be testable so that election officials have confidence that they meet the necessary criteria.

7.) *Transparency*—voters should be able to possess a general knowledge and understanding of the voting process.

8.) *Cost-effectiveness*—election systems should be affordable and efficient.

9.) *Ease of Administration*—the system must be able to be managed at the polling site by polling administrators

10.) ***Intra-County Voting*** – Voters should be able to cast their ballots at any polling site belonging to the county in which they are resident

i. All ballot styles within a county will be available in all polling places within the county

ii. Election officials must be able to authenticate all voters in the county regardless of precinct. To provide voters with the option of voting from multiple locations within a county, poll workers should be given the appropriate tools to authenticate all voters within a county and ensure they are provided the correct ballot.

Security Requirements

1.) ***Eligibility and Authentication***—only authorized voters should be able to vote.

2.) ***Uniqueness***—no voter should be able to vote more than one time.

3.) ***Integrity***—votes should not be able to be modified, forged, or deleted without detection.

a. Internet Voting Machines must be secured from attacks on the operating system. Potential computer attacks include malicious "Virus" or "Trojan Horse" computer code which could affect access to or the integrity of a voter's ballot. In this second stage of Internet Voting, the securing of the machines would be completed by election officials.

4.) ***Secrecy and Non-Coercibility***—no one should be able to determine how any individual voted (other than themselves), and voters should not be able to prove how they voted (which would facilitate vote selling or coercion).

a. The ballot must be encrypted as it travels over the Internet to protect the secrecy and integrity of each vote. (Decision on encryption algorithm(s) pending.)

5.) ***Open Source*** – All source code for the system should be publicly available (given that this project is being done at an academic institution this is unavoidable). Voters have a right to understand as much of the voting process as they are capable.

Requirements our project will focus on

We will focus the bulk of our work on meeting the requirements in **bold**. The other requirements will be assumed to be met and will be simulated. Our project will center on enabling voters to cast their ballots at any polling site in the county (functional requirement FR10). This would require capturing information tying voters to their votes in order to ensure that each voter only votes once. This concept touches upon the idea of functional requirement FR1 as it plays a key role in the accuracy of counts and recounts. This, in turn, causes challenges to arise in security requirements SR1-SR4 that we will address with high priority. Any information linking a voter to a vote immediately begins to infringe upon ballot secrecy; we will design measures to ensure that ballots remain secret in spite of the added functionality (SR4). Work will also be done to design a voter authentication system that supports intra-county voting (SR1). Such a system does not exist currently; lists of eligible voters are currently only maintained per polling site. We will design an architecture that will make it feasible for voter authentication information to be available countywide. This architecture will be impervious to Denial of Service attacks and resistant against locally inserted malicious code (SR3). We will employ encryption techniques during all Internet based transmissions to insure secrecy (SR4a). We feel that functional requirement FR4 is also important for intra-county voting, as each voting site must have access to and be able to use every ballot type available in its county. In the event of a system failure we will devise a suitable backup plan to ensure that the system degrades gracefully (FR3). Also we plan to have all the source code for the project made publicly available (FR5).