BUSINESS REQUIREMENT

DATE	20 SEPTEMBER 2023
TEAM ID	NM2023TMID02213
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM
MAXIMAM MARKS	4 MARKS

Designing a biometric security system for a voting platform involves careful consideration of various technical and non-technical aspects to ensure the security, accuracy, and integrity of the voting process. Below are some business requirements you should consider when implementing a biometric security system for a voting platform:

1. **Regulatory Compliance:**
   - Ensure compliance with local and national regulations related to voting systems and biometric data handling.
2. **Security:**
   - Implement robust encryption mechanisms to secure biometric data during transmission and storage.
   - Use secure authentication protocols to prevent unauthorized access to the voting platform.
   - Employ anti-spoofing measures to detect and prevent the use of fake biometric data.
3. **Accuracy and Reliability:**
   - Conduct thorough testing and validation of the biometric recognition system to ensure accuracy and reliability.
   - Implement redundant systems and backup mechanisms to minimize the risk of system failures.
4. **Scalability:**
   - Design the system to handle a scalable number of users and votes, especially during peak voting periods.

- Ensure that the system can accommodate future expansions and updates.

5. **User Authentication:**
   - Implement multi-factor authentication, combining biometric data with other authentication methods, such as a unique identifier or password.
   - Provide a secure process for user registration and enrollment of biometric data.
6. **Privacy Protection:**
   - Establish strict policies for the collection, storage, and use of biometric data, ensuring compliance with privacy laws.
   - Implement anonymization techniques to dissociate biometric data from voter identity wherever possible.
7. **Usability:**
   - Design a user-friendly interface for both voters and election administrators.
   - Ensure that the biometric recognition process is intuitive and efficient to encourage widespread adoption.
8. **Auditability and Transparency:**
   - Implement an audit trail to record all interactions with the voting platform, including biometric data access and modifications.
   - Provide transparency in the voting process, allowing voters to verify their choices and ensuring that the system is tamper-evident.
9. **Interoperability:**
   - Ensure that the biometric security system can integrate seamlessly with other components of the voting platform, such as voter registration databases and result tabulation systems.
10. **Training and Support:**
    - Provide comprehensive training materials and support for election officials and voters.
    - Establish a helpdesk or support system to address any issues or concerns related to the biometric security system.
11. **Emergency Contingencies:**
    - Develop contingency plans for unforeseen events, such as system failures, cyber attacks, or natural disasters, to ensure the continuity of the voting process.
12. **Accessibility:**

- Ensure that the system is accessible to all eligible voters, including those with disabilities. Implement features such as voice prompts or alternative authentication methods.

Remember to consult with legal experts, cybersecurity professionals, and other relevant stakeholders throughout the development and implementation process to address potential challenges and ensure the overall success of the biometric security system for the voting platform.