LSEP (Legal, Social, Ethical, Professional)

1. Legal Compliance

Our project will adhere to key legal frameworks governing data protection and intellectual property.

- **Data Protection & Privacy Laws:**
  - **PDPA Malaysia Compliance:** The project will strictly comply with the Personal Data Protection Act 2010 (PDPA) of Malaysia.
    - **User Consent:** We will obtain explicit and informed consent from users during registration, clearly stating what data (e.g., student ID, email, card images, NFC UID) is collected and how it will be used solely for access control and identity verification.
    - **Purpose Limitation:** Data collected will be used only for the stated purposes of the NFCampus system and not for any unrelated secondary purposes like marketing, unless separate consent is obtained.
    - **Data Security:** We will implement our own security measures to prevent unauthorized access, disclosure, or breach of personal data.
    - **Data Retention & User Rights:** Users will have the right to access their personal data and request correction or account deletion.

- **Licensing, Copyright, and Intellectual Property:**
  - **Third-Party Libraries:** We will use open-source libraries (e.g., Google's ML Kit for OCR) under their respective licenses (like Apache 2.0). We will ensure compliance by including all required copyright notices and license terms in our application's documentation.

    - **University Intellectual Property:** The student card design and logo are the intellectual property of the university. Our app's use of card images via OCR is for functional data extraction only, and shall not be used for replication or misuse of the card's branded design.

- **Permissions and Safety Regulations:**
    - **App Permissions:** The Android application will explicitly request only the necessary permissions. Users will be informed why each permission is needed to allow transparency.

---

2. Ethical Guidelines

We are committed to ensuring our project operates with high ethical standards, prioritizing user welfare and fairness.

- **Fair Treatment of Users:**
    - The system is designed to be inclusive for all students with compatible Android devices and a valid university card. We acknowledge the potential exclusion of iOS users and students who lose their physical cards before registering, and we recommend the physical card system remain as a necessary backup.

- **Avoiding Harm:**
    - **Bias and Discrimination:** The primary risk of bias lies in the potential for higher failure rates with damaged or non-standard cards. The manual correction fallback is a critical feature to mitigate this and prevent harm or frustration from technical errors.

    - **Security Harm:** A core ethical duty is to protect users from the harm that would result from a security breach. By implementing strong MFA and secure backend practices, we actively work to prevent unauthorized access and impersonation, which could lead to security incidents or reputational damage for the user.

- **Transparency and Honesty:**
    - We will provide a clear, easily understandable Privacy Policy that explains data collection, usage, and storage practices in plain language. The system's capabilities and limitations will be honestly communicated to users to manage expectations.

- **Confidentiality:**
    - All user data, especially the scanned card images and the unique NFC UID, will be treated as confidential information. Access to this data on the backend will be strictly restricted to what is necessary for system administration and troubleshooting. It will never be sold, shared with third parties, or used for any purpose beyond the core function of the application without explicit user consent.

---

3. Social Impact

Our project, NFCampus, is designed to create a positive and transformative impact within the university community by modernizing student identity verification. We aim to enhance daily campus life while proactively addressing potential social challenges.

- **Positive Impacts**

  - **Enhanced Convenience and Efficiency:**
    - The primary social benefit is the significant increase in convenience for students. By consolidating their physical student ID into their smartphone, students no longer need to carry an additional card. This streamlines access to facilities, library services, and event check-ins, reducing wait times and making campus interactions more efficient.

- **Potential Negative Impacts and Mitigation**
  - **Digital Divide and Exclusion:**
    - **Impact:** The system could inadvertently exclude students who do not own a compatible Android smartphone, particularly iOS users. It also presents a barrier for students who lose their physical card before registering on the app, potentially locking them out of essential services.

    - **Minimization:** We explicitly do not propose replacing the physical card system. Instead, we advocate for it to remain as necessary and fully supported backup. This ensures that no student is disadvantaged due to their device type or a temporary situation. Clear communication will emphasize that digital ID is an optional convenience, not a mandatory replacement.

- **Target Beneficiaries**
  - The primary beneficiaries of the NFCampus system are university students, who gain a more convenient, secure, and modern method of managing their campus identity. Secondary beneficiaries include university administration and staff, who benefit from increased operational efficiency, reduced costs associated with card replacement, and an enhanced overall security posture on campus.

---

4. Professionalism

Our team will maintain a high level of professionalism throughout the project. We commit to producing quality work through proper testing, documentation, and use of best practices such as version control and peer reviews. We will follow a weekly progress schedule to ensure deadlines are met and maintain clear communication within the team and with supervisors.

All reports and updates will be accurate and transparent, and any issues will be promptly communicated. Each member is responsible for their assigned tasks, and the team will uphold accountability, ethical conduct, and respect for user confidentiality at all times.

---

5. Risks

- **Technical Risks**
  - **Bugs or System Errors:** May affect performance. *Mitigation:* Regular testing and reviews.
  - **Device Compatibility:** NFC may not work consistently on all phones. *Mitigation:* Test on multiple devices and keep physical card backup.
  - **OCR/NFC Failures:** Damaged cards or poor scans can cause errors. *Mitigation:* Allow manual correction.

- **Operational Risks**
  - **User Onboarding Issues:** Users may struggle with setup. *Mitigation:* Provide clear instructions and tutorials.
  - **Server Downtime:** Backend failures may disrupt access. *Mitigation:* Use reliable cloud hosting and backups.

- **Financial Risks**
  - **Cloud Costs Increasing:** Higher usage may raise hosting fees. *Mitigation:* Monitor usage and optimize resources.
  - **Maintenance Costs:** Ongoing support may require a budget. *Mitigation:* Provide cost estimates for future planning.

6. Sustainability

Our project, NFCampus, is designed not just as a short-term solution but as a sustainable and evolving platform that supports environmental goals, long-term usability, and future growth.

- **Environmental Sustainability**
  - **Reduction of Physical Waste:**
    - The most direct environmental contribution is the significant reduction in plastic waste. By providing a digital alternative to the physical student ID card, we directly decrease the demand for new card production. This mitigates the environmental impact associated with the manufacturing, packaging, and shipping of thousands of PVC cards over time. Furthermore, it reduces the waste generated from lost, damaged, or expired cards that need to be repeatedly reprinted.

  - **Promoting a Paperless Ecosystem:**
    - The system digitizes the identity verification process, eliminating the need for paper-based sign-in sheets, manual attendance logs, and physical forms for access to various campus services. This contributes to a broader reduction in paper consumption across the university.

- **Long-Term Usability**
  - **Device-Agnostic Core Principle:**
    - The system's core functionality—verifying a user via a unique identifier (NFC UID)—is independent of specific phone models or operating systems. While the initial rollout targets Android, the architecture is designed to allow for a future iOS version without rebuilding the entire backend, ensuring the system remains relevant as personal technology evolves.

  - **Adaptable to Changing Needs:**

        - The digital identity framework can be expanded beyond simple access control. It can be adapted to integrate with new university initiatives, such as digital wallets, event ticketing, or public transport passes, ensuring the platform remains valuable and in use for years to come.

- **Maintainability and Scalability**
    - **Modular and Well-Documented Codebase:**
        - The project is built with a modular architecture, separating key components (OCR module, NFC module, backend API, database). This allows developers to update, debug, or replace one module without affecting the entire system. Comprehensive documentation will be maintained to ensure long-term understandability for future development teams.

    - **Scalable Cloud-Based Backend:**
        - The system will use cloud hosting (e.g., AWS, Google Cloud, or Azure), which provides inherent scalability. As the student population grows or usage spikes during peak times (e.g., class changes), the backend can automatically allocate more resources to maintain performance, avoiding service degradation or downtime.

---

7. Continuity

To ensure the project's value extends beyond the initial development phase, we have developed a clear continuity plan.

- **Maintenance Plan**
    - The final documentation will include a detailed "Maintenance Guide" which covers the system architecture, deployment process, and troubleshooting steps for common issues.

- **Future Updates and Improvements**
    - The project backlog includes items explicitly marked for future work such as iOS development and admin dashboard which can be handed over to future student teams or the campus's IT department for further development.

- **Cost Planning**
    - Understanding ongoing operational costs is crucial for long-term sustainable operation. The main costs associated with NFCampus after deployment are related to cloud hosting and services. We recommend the following structure:
        - **Institutional Deployment:** For campus to adopt the system, the main cost would be a predictable monthly or annual fee for backend hosting such as Firebase or Google Cloud, which is based on user count and data usage.
        - **Maintenance Labor:** Campus would need to allocate a budget for IT staff for daily monitoring, updates, and user support.

    - We will provide an initial cost estimate based on the resource usage of the prototype system to facilitate campus development and a budget for full rollout.

- **Handover Documentation**
    - All source code, system design documents, API documentation, and the maintenance guide will be compiled, packaged, and submitted to our mentors. This is to provide a complete blueprint for the project's future development.