**System/Hardware Requirements-** The password manager has minimal requirements, as it works on any computer that can install the Python library. To use the Cloud feature, you first need to set up a Google account with Google Drive. When storing a password, it will direct you to Google, where you can select your account or create one if you don't already have one.

**Ethical/ Legal and Security Concerns-** While our app adheres to ethical and legal standards, it does present notable security limitations. It was not developed to provide enterprise-level or high-security protection. Although passwords are stored using basic encryption methods, the implementation lacks the robustness needed to prevent decryption by individuals with advanced knowledge of password-cracking techniques. As such, we do not recommend relying on this application for safeguarding sensitive credentials. Instead, it is intended as a simplified demonstration of how a password manager functions, serving educational or conceptual purposes rather than secure, real-world usage.

**Project Performance, Uniqueness, and Similarity to Others -** Our app performs as intended. A simple password manager app was created as a proof of concept to demonstrate the fundamentals of secure credential storage and user authentication. The primary goal was to explore encryption techniques and user interface design in a controlled development environment. It served as a learning tool or prototype rather than a fully deployed product, lacking the rigorous security auditing, compliance certifications, and scalability features necessary for real-world use. Because it was not intended to handle sensitive user data outside of testing scenarios, it remained a conceptual project without exposure to live users or production environments. Our application takes a unique approach by utilizing Google Drive for password storage instead of a traditional database. This decision was driven by the goal of simplifying implementation while ensuring cross-device accessibility. By leveraging Google Drive’s cloud infrastructure, we enabled users to securely access their stored passwords from any device with an internet connection, streamlining the user experience without the complexity of managing a custom backend database. This method also allowed for easier integration within the scope of our project, aligning with our focus on accessibility and ease of use.

Before beginning development, we conducted research on leading password managers such as NordPass and 1Password to gain insight into industry standards and functionality. Through this comparison, we identified key features that make these platforms robust and user-friendly, including cloud-based database systems and seamless browser integration. However, given the scope of our project and the limited time and resources available, implementing such advanced capabilities was not feasible. Instead, we focused on achievable goals, such as designing a clean, intuitive user interface and enabling cross-device accessibility. While our app does not yet include the full range of enterprise-level security features, it reflects a thoughtful balance between functionality and practicality within the constraints of our development environment.