Technical Description	
Encryption	AES-128 Advanced Encryption Standard
Standards, Security protocols	Meets the requirements of ISO 27001, SOC, the PCI Data Security Standard, Fed RAMP, the Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584).
Vulnerability	Secure from known vulnerabilities
Cloud solution	Cloud solution via AWS (Amazon Web Services) which consist of one or more data centres, each with redundant power, networking and connectivity, housed in separate facilities. Amazon engineered Availability Zones that are designed to be insulated from failures in other availability zones. Availability zones do not share the same infrastructure. Applications running in more than one availability zone can achieve higher availability.
Database & Servers	RDS service from AWS. AWS RDS is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. RDS is encrypted instances use the industry standard AES-256 encryption algorithm to encrypt the data on the server.
Data & Information Security: Users, Content	Authentication token for user access authentication for almost every backend request user sends out from client app (except sign up, login, change password). All user passwords are stored using PBKDF2WithHmacSHA1 algorithm instead of plain text. The web admin or developers in UAN-Backend cannot decrypt user's password. Information is stored in a secure cloud environment and the user owned data is always transmitted using encryption. Application data access and deletion is possible by user only. User is the only owner of content posted on the platform and is in full control of data.
Location Information: Users, Content	App uses location information via GPS/location services of the device. Adequate safeguards are in place to protect privacy and confidentiality for location services and user can choose if they want to show their position or not when posting in the platform, responding to other users or posting an alert. Location information is not being gathered and that data is not transmitted, nor stored, or both, without users knowledge. The location information is fetched from the user phone and needs user confirmation and approval. User can at any time disapprove the application from receiving location information however the location data is vital to the functionality of the application and the user experience.
API	API connection might be used for certain clients and community development projects. All API connections with the platform are secured with the highest industry standards.