ArriveAlert: Destination Notifier App Security Policy

Effective Date: December 2, 2024

Policy Statement

ArriveAlert is committed to ensuring the confidentiality, integrity, and availability of user data. This policy outlines the practices and responsibilities to protect user authentication, shared locations, and destination data from unauthorized access, breaches, and vulnerabilities.

Scope

This policy applies to all users, developers, and third-party integrations (e.g., Firebase, Google Maps API) used within the ArriveAlert application.

Security Objectives

1. Ensure user data, including authentication tokens and shared locations, is kept confidential.
2. Protect against unauthorized access to user locations or credentials.
3. Comply with industry best practices for data encryption and secure storage.
4. Educate developers and testers on secure coding practices.

Responsibilities

1. **Management**

- Ensure that all security measures are implemented during the app's development.
- Allocate resources for regular security reviews and updates.

2. **Developers**

- Encrypt sensitive user data, such as locations and authentication tokens.
- Conduct security testing to identify and mitigate vulnerabilities.
- Implement strong access control mechanisms for the database and app features.

Access Control

1. **Authentication**

- Use Firebase Authentication for secure Google and Facebook logins.
- Require multi-factor authentication (MFA) for sensitive operations, if feasible.

2. **User Permissions**

- Only allow users to access their own location and shared data.
- Restrict admin-level access to developers for debugging and support purposes.

Data Protection

1. **Encryption**

- Encrypt data during transmission using HTTPS and Firebase's built-in encryption mechanisms.
- Encrypt sensitive fields (e.g., location coordinates) in the database.

2. **Backup**

- Implement automated backups for user-shared locations and settings in Firebase.

Incident Response

1. **Detection**

- Use Firebase monitoring tools to detect anomalies, such as unauthorized access attempts.

2. **Response**

- Immediately revoke compromised authentication tokens.
- Notify affected users and secure impacted systems.

3. **Recovery**

- Review the incident and implement measures to prevent recurrence.

Training and Awareness

Developers must follow security best practices, such as:

- Avoiding hard-coded credentials.
- Using Firebase's rules for database access.

Compliance

Align with:

- Firebase security standards.
- Google Maps API terms of service.
- Applicable data privacy laws, like GDPR, if targeting users in specific regions.

Enforcement

Violations of this policy by developers or testers may result in revocation of access rights or legal consequences.

Review and Revision

This policy will be reviewed annually or after any security incident to ensure its effectiveness.

Approval:

ABRAHEM P. ANQUI

Capstone Advisor

November 29, 2024