Marquis Technologies - Mobility and/or Field Testing Security Policy

Function : Corporate Security

Approver : Deven Potdar

Version & Status : 1.1, Approved

Revision History

Version	Reviewer	Date
1.0	Deven Potdar	6th June 2023
1.1	Sudharshan K	11th June 2024

1. Purpose

This policy establishes guidelines and protocols to ensure the security, confidentiality, and integrity of unlaunched mobile phones during field testing. It aims to protect sensitive information, prevent unauthorized access, and mitigate risks associated with handling pre-release devices.

2. Scope

This policy applies to all employees, contractors, and drivers involved in mobility testing or field testing of unlaunched mobile phones.

3. Policy Guidelines

1. Authorization and Access

Only authorized personnel are permitted to handle and transport unlaunched mobile phones for field testing.

Each individual must sign a confidentiality agreement and acknowledge understanding of the security protocols before accessing the devices.

2. Device Handling

Devices must be stored in secure, tamper-proof containers (Bags or Briefcase) during transport.

Employees must carry only the required number of devices for the testing assignment and avoid bringing unnecessary devices or equipment.

Devices must not be left unattended in vehicles, public places, or unsecured areas.

3. Data Security

Pre-release devices must have security measures enabled, such as device encryption, PINs, or biometric locks.

Employees must not download or store personal data on the test devices.

Field test data should be transmitted securely through encrypted channels to authorized servers or systems.

4. Prohibited Activities

Testing activities must not occur in public places where devices can be exposed to unauthorized observation or photography.

Employees are strictly prohibited from using the devices for non-work-related purposes or sharing device details with unauthorized individuals.

Avoid testing during national events like Election Day.

5. Incident Reporting

Any loss, theft, or tampering of test devices must be reported immediately to the project manager and security team.

Employees must provide a detailed account of the incident, including the last known location of the device and steps taken to recover it.

6. Transport and Logistics

Devices must be transported via secure means, with tracking enabled wherever possible.

When transferring devices between employees or teams, a proper check-in/check-out protocol must be followed, including acknowledgment receipts.

7. Location and Environment

Field testing should be conducted only in pre-approved locations with minimal risk of loss or exposure.

Employees must avoid high-risk environments, such as crowded public areas or locations with a high likelihood of theft.

There should not be any Field Testing on any Political events (i.e. Elections) or National holidays

8. Training and Awareness

All employees involved in field testing must undergo mandatory training on security protocols, handling procedures, and incident response.

Refresher training sessions should be conducted periodically to reinforce best practices.

Drivers also need to go through Information Security training.

9. Recovery and Investigation

In the event of a security breach, the company's security team will initiate an investigation to determine the root cause and implement corrective measures.

Testing activities may be suspended temporarily if required to ensure device security.

10. Enforcement

Violations of this policy may result in disciplinary actions, including termination of employment or contract, and potential legal consequences.

Employees are encouraged to report any suspected or actual breaches of this policy without fear of retaliation.

11. Review and Updates

This policy will be reviewed and updated annually or as necessary to address emerging threats and changes in operational requirements.