Mobile Application Security Guidelines – OWASP MASVS Compliance

Organization: LKP Securities Ltd.
Application Name: Get Set Grow
Document Version: 1.0
Prepared By: Development / IT Security Team
Reviewed By: IT Head / Compliance Team
Date: 14-01-2026

1. Objective

The objective of this document is to confirm that OWASP security guidelines, including the OWASP Mobile Application Security Verification Standard (MASVS), are referred to and followed during the mobile application development lifecycle to ensure secure design, development, and deployment in line with SEBI CSCRF requirements.

2. Reference Standard

- OWASP Mobile Application Security Verification Standard (MASVS)
- OWASP Mobile Top 10

3. Scope of Security Controls

MASVS Security Area	Controls Implemented
Authentication & Session Management	Secure login, session timeout, token protection
Authorization	Role-based access control
Data Storage Security	Encryption of sensitive data
Network Communication	Secure API communication using HTTPS/TLS
Platform Interaction	Secure usage of OS-level features
Code Quality & Build	Secure coding practices and reviews
Resilience	Protection against tampering and reverse engineering

4. Secure Development Lifecycle Integration

OWASP security guidelines are integrated into the software development lifecycle (SDLC), including design, development, testing, and pre-production review stages.

5. Validation & Review Activities

- Secure code reviews
- Manual and automated security testing
- Pre-release security compliance checks

6. Compliance Statement

The mobile application security controls implemented are aligned with OWASP MASVS guidelines and support compliance with SEBI Cyber Security and Cyber Resilience Framework (CSCRF).

7. Approval & Sign-off

Name	Role	Signature	Date
Ashish V Dwivedi	Delivery Manager		14-01-2026