Appx C
(Ref para 11 of DDG IT letter No B/04001/Policy/Sw/DDG IT(T&P) Dt as in Digital Sign)

CHECKLIST FOR PHONE SHIELD SOFTWARE

S.No	Mandatory Details	Remarks
01.	Name of Proj (inc ver)	Phone Shield
02.	Name of Sponsor.	Nil
03.	Type of SW(Bespoke/COTS/Customized)	Bespoke
04.	Brief Justification/endorsement on reqmt for devp of Sw appl.	The proposed sw appl is essential to address the critical need for detecting and managing banned mobile appls across the org. Currently, the absence of an automated solution exposes the org to potential risks, incl security breaches, data leaks, and non-compliance with org policies. By implementing this solution, the org will benefit from: **1. Enhanced Security:** Proactive detection and removal of unauth appls will minimize vulnerabilities and safeguard sensitive data. **2. Improved Compliance:** Ensures adherence to org policies and requirements by monitoring and controlling appl usage. **3. Op Efficiency:** Automates the detection process, reducing the need for manual monitoring and improving accuracy. **4. Centralized Monitoring and Reporting:** Provides a unified platform for tracking compliance, generating reports, and enabling swift decision-making. The proposal aims to create a secure, compliant, and efficient environment by leveraging a robust sw appl that meets the org growing tech and security demands.

S.No	Mandatory Details	Remarks
05.	Aim, Scope and Purpose incl utility, beneficiaries and tgt users.	**Aim:** The aim of the proposed appl is to develop an automated sys for detecting and managing banned mobile appls across the org. This will ensure compliance with org policies, strengthen security, and streamline the monitoring process. **Scope:** The scope of the sw includes: 1. Automated Detection: Identifying banned or unauth mobile appls installed on devices. 2. Whitelisted Appl Mgt: Ensuring only approved appls are allowed within the org envt. 3. Centralized Monitoring and Reporting: Providing a dashboard for real-time tracking, reporting, and alerts. 4. Scalability: Deployable across the entire org, applicable to all Android users. 5. Integration: Seamless integration with the existing IT infra for smooth operations. **Purpose:** The purpose of the proposed sw appl is to: 1. Enhance org security by eliminating unauth and banned appls. 2. Ensure adherence to regulatory and internal compliance policies. 3. Automate monitoring processes to reduce manual effort and errors. 4. Provide actionable insights through centralized reporting and analytics for decision-making. **Beneficiaries:** 1. Org as a Whole: Ensures a secure and compliant envt. 2. IT and Compliance Teams: Simplifies monitoring, reporting, and enforcement processes. 3. Management: Improves oversight and policy impl across departments. 4. Manpower: Provides clarity on permissible appls, reducing inadvertent violations of policy. **Utility:** 1.The sw appl will serve as a robust solution to:

S.No	Mandatory Details	Remarks
		2. Protect org data and infra from potential risks posed by unauthorized appls. 3. Ensure compliance with standards and org policies. 4. Optimize resource utilization by automating processes and reducing manual intervention. 5. Enable proactive detection and prompt action through real-time alerts and reporting. 6. Overall, the sw will act as a key tool to strengthen the org security posture, improve op efficiency, and sp policy enforcement.
06.	To be hosted on internet/ADN with brief justification.	For provn of real time alerts and notification, the appl will be hosted in internet.
07.	Being devp in house or through IT Funds.	In house devp.
08.	Usability of proposed appls by other Arms/services/org/est.	One appl per fmn will be used for real time monitoring.
09.	HW and IT infrastructure reqd in the form of Virtual Machines at Data Centre (incl memory, storage and processing capabilities).	NA
10.	Brief details of content of the proposed Sw appl.	The proposed sw appl will include the following key components: **1. Automated Appl Detection:** Scans and identifies banned or unauth mobile appls across devices within the org. **2. Whitelist Mgt:** Maint and enforces a list of approved appls to ensure compliance with org policies. **3. Centralized Dashboard:** Provides a unified interface for admins to monitor appl compliance, generate reports, and view real-time status. **4. Reporting and Alerts:** Generates reports on non-compliant devices or appls and sends automated alerts to designated stakeholders for quick action. **5. User and Device Mgt:** Tracks all devices connected and associates them with user profiles for accountability. **6. Security and Compliance Features:** Ensures adherence to org security policies by preventing the installation or use of banned appls.

S.No	Mandatory Details	Remarks
		7. Scalability and Integration: Designed to scale across the entire org and integrate seamlessly with existing IT infra. This software application will provide a comprehensive solution to detect, manage, and enforce compliance regarding mobile appls, enhancing security and op efficiency.
11.	Endorsement by Head of Br/ Svc/ Fmn.	NA
12.	Details of user base.	The appl will be applicable to all Android users across the org, including all hierarchies. It will cover the entire user base utilizing mobile devices.
13.	Envisaged cost of entire proj incl licence fees and maints	Devp cost Nil Maint cost 5000 (for domain annual fees and hosting)
14.	Projected dt of completion incl majn timelines.	June 2024.
15.	Brief details of SW platform and tech stack proposed for devp of appl incl op sys dependencies (if any).	Laravel Framework (Based on PHP) HTML, CSS Java Script for Front End MySQL for Database Java for Client Mobile Appl
16.	Brief details of proposed network and bandwidth reqmts.	Bandwidth depends on number of clients
17.	Brief details of OS and Sys software reqmt.	Supports for all version of Android.
18.	Brief Details of proposed data security measures incl backup of data.	XSS protection LFRI protection MITM protection Input Validation & Sanitisation API authentication
19.	Brief Details of Proposed Database Engine to be used in the Appl.	MySQL 8.0 Database Engine
20.	Details of SW architecture and COTS SW proposed to be utilised.	Model View Controller (MVC) Architecture impl on Laravel
21.	Details of SW architecture - Centralised /Federated/Hybrid.	Centralised
22.	Brief Details of proposed utilisation of Public Key Intra (PKI) and Iden and Access Mgt (IAM).	Username Password based authentication & API authentication
23.	Technology dependencies (if any).	Nil
24.	Database Reqmt.	MySQL 8.0 Database Engine
25.	Enhancement/upgradation (incl patch mgt /SW updt procedure and mechanism.	Patch upgradation & Android build release
26.	Details of licencing (if any).	Nil