Annexure A: Scope of Work - MDM Solution

An MDM (Mobile Device Management) solution is designed to manage and secure mobile devices within our organization. A cloud solution that should be able to manage 2000 devices over a thirty-six (36) month period; the MDM solution must be capable of handling a large number of devices and providing comprehensive device management features.

The MDM solution should provide centralized control and management of all devices, including smartphones, tablets, and laptops, regardless of the operating system. It should offer remote device configuration, application deployment, and policy enforcement to ensure consistent security and compliance across all devices.

In addition to device management, the MDM solution should include the following comprehensive technical specifications:

- **Platform Support**: ability to support multiple operating systems such as Android, iOS, Windows, macOS and HarmonyOS.
- **Device Enrollment**: The solution should provide a simple and secure process for enrolling devices, to be done via app or web portal.
- **Device Management**: The solution should provide a range of device management features such as remote lock, wipe, and passcode reset.
- **App Management**: The solution should allow IT admins to distribute, manage, and secure mobile apps across all devices. It should also allow for blacklisting or whitelisting apps.
- **Policy Management**: The solution should allow for the creation and enforcement of policies that ensure compliance with security and regulatory standards.
- **Reporting and Analytics**: The solution should provide detailed reporting and data analytics to track device usage, app adoption, and security events.
- **Integration**: The solution should integrate with other IT systems such as identity and access management solutions, helpdesk systems, security information and event management systems.
- **Security**: The solution should employ strong security measures to protect sensitive data on mobile devices. This includes encryption of data at rest and in transit, secure boot, and device-level VPN.
- **Scalability**: The solution should be scalable to accommodate a growing number of devices and users.
- **User Experience**: The solution should provide a seamless user experience for employees, allowing them to access their apps and data securely from anywhere.

- **Define a BYOD Policy**: Establish a clear policy that outlines the acceptable use of personal devices for work purposes. This should include guidelines for security, data protection, and acceptable use.
- **Restrict users to access emails from untrusted / non managed devices**: Implement an MDM solution that allows you to manage and secure devices that access email. It must enforce policies that require devices to be encrypted, have a passcode, or prohibit certain activities such as jailbreaking.
- **Remote Control**: The solution must include software that allows administrators to remotely access and control managed devices. With remote control, administrators should be able to view the device screen, take screenshots, and perform actions such as installing or removing apps, changing settings, or restarting the device.
- **Mobile Device Location Tracking**: Mobile Device Management (MDM) solutions must further include mobile tracking features that allow administrators to track the location of managed devices. The location data must be transmitted to the MDM server, where it can be viewed by administrators.
- **Security Standards**: The platform should adhere to security standards such as SSL/TLS encryption, two-factor authentication, and data encryption to protect sensitive data and prevent unauthorized access.
- **Compliance Standards**: The Solution should comply with various regulations such as GDPR, POPI, and other data compliance standards
- **User Authentication Standards**: The platform should support various user authentication standards such as LDAP to ensure secure access to enterprise data
- **Containerization**: The solution should be able to create a Secure Container or Workspace on the Device, which is Isolated from the rest of the Devices Operating system and data. The container should be controlled by the MD solution and can be configured with specific security policies, such as password requirements, data encryption and remote wipe capabilities.