Document 3.1: Mobile Device Management, Unlocking, and Theft Protocols

Filename: `OPS_2025_Mobile_Device_Security_SOP.pdf`

1.0 STATUTORY DEVICE UNLOCKING STANDARDS As of 2025, all mobile handsets and tablets sold through official retail or corporate channels must be **unlocked by default** at the point of sale.

- **Prohibition of Fees:** Service providers are strictly prohibited from charging "Unlocking Fees."
- **Legacy Devices:** For hardware sold prior to current regulations, agents must provide unlocking codes upon request without requiring the customer to have an active account, provided the device is not flagged as stolen.

2.0 LOST OR STOLEN DEVICE PROTOCOL (LSP) Upon notification that a mobile device is lost or stolen, the following mandatory actions must be executed:

- **Immediate Suspension:** The Service Provider must suspend the customer's service **at no charge** immediately upon report.
- **Liability Cap:** The customer remains liable for all charges incurred *before* the report. After the report is logged, the customer is not responsible for any unauthorized voice, text, or data usage.
- **Blacklisting (IMEI):** The agent must offer to add the device’s **IMEI (International Mobile Equipment Identity)** to the national blacklist to prevent the device from being activated on any other domestic carrier network.

3.0 RESTORATION OF SERVICE If a device is recovered, the service must be restored at no cost. The agent must verify the customer’s identity via **Two-Factor Authentication (2FA)** before removing the IMEI from the blacklist or re-enabling the SIM/eSIM.

4.0 5G SIM & eSIM CONFIGURATION

- **APN Standards:** All devices must use the `internet.telecomcorp.pro` APN for 5G Ultra-Wideband access.
- **eSIM Provisioning:** eSIMs must be delivered via a secure QR code or direct "Push to Device" via the provider app. Manual entry of SM-DP+ addresses is discouraged for security reasons.