NYCPS TMS: Prescriptive Hardware Lifecycle & Logistics Management Strategy

I. Introduction: The Physical Foundation & Operational Challenge

This document mandates the hyper-detailed, prescriptive strategy for managing the complete physical lifecycle of all hardware components essential to the NYCPS Transportation Management System (TMS). This includes approximately 11,000+ core mobile devices (GPS-enabled tablets/phones), plus associated peripherals (vehicle mounts, chargers, potentially QR code scanners, protective cases) and the physical QR/Barcode key tags for students. Managing this vast inventory across ~60+ School Bus Contractor (SBC) depots and potentially ~9,500+ vehicles represents a significant logistical and operational challenge requiring absolute rigor, security, efficiency, and accountability.

This strategy details the non-negotiable processes, controls, tools, roles, and compliance requirements governing hardware from procurement and initial acceptance testing through secure warehousing, inventory tracking, configuration (kitting), distribution, installation, ongoing maintenance (firmware, battery), break-fix/RMA support, loss/theft response, and ultimately, certified secure disposal at end-of-life. It integrates tightly with the overall project plan, vendor management, security, financial, and support strategies.

> **Failure to manage hardware logistics effectively can lead to significant deployment delays, operational disruptions (buses without functional devices), security vulnerabilities (lost/stolen devices with data), inflated costs (lost inventory, inefficient repairs), compliance failures (improper disposal), and damage to relationships with crucial SBC partners.**

II. Hardware Logistics Governance & Roles

Clear ownership and defined roles are critical for managing the physical asset lifecycle.

> ***Implementation How-To:***
>
> 1. Establish dedicated roles within the project/operational structure:

- **Hardware Logistics Lead (Dedicated Role):** Owns and executes this entire strategy. Manages inventory system, coordinates warehousing/distribution, oversees kitting/preparation, manages RMA process, tracks hardware KPIs, primary POC for hardware vendors and SBCs regarding logistics. Reports to PM.**

- **Inventory Manager (Can be part of Logistics Lead role):** Responsible for maintaining the accuracy of the central inventory system, conducting physical audits/reconciliations, managing buffer stock levels, generating inventory reports.**

- ****Field Technician Coordinator (Can be part of Logistics Lead or Vendor Mgmt):** Schedules and coordinates device installation, de-installation, and on-site break-fix activities with SBCs and field technicians (whether vendor or

internal). Tracks completion via ticketing system.

- ****Hardware Vendor Manager (Likely part of overall Vendor Mgmt):** Manages the contractual relationship and performance (SLAs for delivery, repair, warranty) of primary hardware suppliers. Handles escalations related to vendor performance.**
- ****Security Team:** Defines security requirements for device hardening, MDM policies (if used), data wipe procedures, and secure disposal standards. Audits compliance.**
- ****DevOps/MDM Admin:** Manages Mobile Device Management (MDM) platform configuration, policy enforcement, remote wipe/lock commands, OS/Firmware update deployment orchestration.**
- ****SBC Point of Contact (POC):** Designated individual at each SBC**

depot responsible for receiving/distributing devices, managing local swap stock, reporting issues, coordinating installations/repairs for their fleet.

- **OPT Asset Management Liaison:** Ensures alignment with overall NYCPS asset management policies and reporting requirements.
- **Finance Liaison/Procurement:** Manages POs for hardware purchases/leases, processes hardware-related invoices based on Logistics Lead validation.

2. Document these roles and their specific responsibilities within the project RACI matrix and relevant process documents in Confluence.
3. Hardware logistics status, KPIs, and risks will be standing items in Weekly Project Status meetings and reported in MBRs.

Responsibility: Project Management, Operations Leadership.

III. Hardware Lifecycle Stages: Prescriptive Processes

Each stage of the hardware lifecycle requires specific, documented, and controlled procedures.

A. Stage 1: Procurement, Specification & Vendor Acceptance Testing (VAT)

1. Detailed Hardware Specification Definition

Implementation How-To:

1. **Develop hyper-detailed technical specification documents for *all* hardware components (mobile device, case, mount, charger, scanner, QR tags) based on RFP requirements, architectural needs, and operational context (NYC environment, vehicle types).**
2. ****Mandatory Mobile Device Specs:****

- **Ruggedness:** Define specific standards (e.g., MIL-STD-810G for drop/shock/vibration, IP67/IP68 for water/dust ingress).
- **Operating System:** Specify required Android/iOS version range, commitment from vendor for OS security updates (aligned with RFP 3.21.1), potential for MDM control. GovCloud compatibility considerations.
- **Security:** Hardware encryption support, secure boot capabilities, compatibility with MDM policies (remote wipe/lock), physical security features (e.g., Kensington lock slot if applicable).
- **Battery:** Define minimum battery life requirement under expected usage patterns (GPS active, screen on, app running) to cover full shifts without mid-

shift charging. Specify battery health reporting capability (if available). Define expected battery lifespan (e.g., >3 years under normal use).

- ****Connectivity:** Cellular (specify required bands for NYC carriers, 4G LTE minimum, 5G readiness?), Wi-Fi (specify standards), Bluetooth (for potential scanner/OBD connection).**
- ****GPS:** High-sensitivity GPS chipset with fast TTFF (Time To First Fix) and good accuracy in urban canyon environments. Support for assisted GPS (A-GPS).**
- ****Display:** Minimum size, resolution, mandatory touchscreen, high brightness/anti-glare for daylight visibility, auto-brightness adjustment.**

- **Processing/Memory:** Sufficient CPU/RAM to run TMS Driver App and OS smoothly without lag (define benchmarks based on app testing).
- **Camera/Scanner:** If device camera used for QR scanning, specify minimum resolution/autofocus capabilities. If external scanner used, specify interface (USB/Bluetooth), scan speed/reliability, barcode types supported (QR mandatory).
- **Peripherals:** Specify requirements for rugged protective cases, secure vehicle mounts (adjustable, lockable?, compliant with NYDMV regs), reliable vehicle chargers (appropriate voltage/connector, fuse protection).

3. Incorporate specifications into RFQ/RFP documents for hardware procurement.

Responsibility: Hardware Logistics Lead, Cloud Architect, Mobile Dev Lead, Security Team.

2. Vendor Selection & Contractual Requirements

Implementation How-To:

1. **Evaluate hardware vendors based not only on cost but critically on: supply chain reliability/capacity (ability to deliver 11k+ units), warranty terms (minimum 3 years preferred, covering defects/normal wear), defined RMA process and turnaround time SLAs, support for OS/firmware updates, proven experience with large-scale deployments, ability to meet customization/kitting needs.**
2. **Contract *must* include: Detailed specifications, firm delivery schedules aligned with project rollout, warranty terms, mandatory RMA SLAs (e.g., <5 business day repair/replace turnaround post-receipt), penalties for SLA breaches, secure packaging/shipping requirements, support for EoL notification and potentially disposal.**

Responsibility: Procurement Liaison, Contract Manager, Hardware Logistics Lead, Legal (OLS).

3. Vendor Acceptance Testing (VAT) - Mandatory

Implementation How-To:

1. **Define a rigorous VAT plan *before* receiving initial hardware shipments. Store plan in Confluence.**
2. ****Sample Selection:** Test a statistically significant sample size from the first large batch(es) received (e.g., 5-10% of initial 1000 units).**
3. ****VAT Checklist (Detailed):****
    - **Physical Inspection: Check for damage, correct model/peripherals, all components included.**
    - **Basic Functionality: Power on/off, screen responsiveness, button operation, charging verification.**

- **OS/Firmware Version Check: Verify matches specified version.**
- **Connectivity Tests: Wi-Fi connection, Cellular connection (SIM insertion/activation if needed, signal strength check), Bluetooth pairing (with scanner if applicable).**
- **GPS Test: Verify quick GPS lock acquisition (TTFF target), location accuracy check (compare against known point).**
- **Camera/Scanner Test: Verify QR code scanning speed and accuracy under various lighting conditions.**
- **TMS Driver App Test: Install/verify pre-installed app launches, basic login test, background operation check.**
- **MDM Enrollment Test (If applicable): Verify successful**

enrollment and policy application.

- **Battery Test (Sampled): Perform basic charge/discharge cycle test on a subset of VAT units to verify initial battery health against spec. (More extensive battery testing might occur during initial tech selection).**
- **Durability Test (Sampled - Optional, Destructive): Potentially perform standardized drop tests on a very small number of units if ruggedness is a major concern and not sufficiently certified by vendor.**

4. **Execution:** Dedicated QA/Logistics team members execute VAT checklist on sampled units. Document results meticulously per serial number.
5. **Acceptance Criteria:** Define clear pass/fail criteria (e.g., <1% DOA rate, <3% failure rate on key functional tests).

6. **Reporting & Remediation:** Report VAT results to Vendor Manager/PM. If failure rate exceeds threshold, reject batch and invoke contractual remedies with vendor. Use findings to refine ongoing QC processes.

Responsibility: QA Lead/Team, Hardware Logistics Lead, Vendor Manager.

Quality Gate: Formal VAT sign-off required before accepting major hardware shipments into inventory.

B. Stage 2: Secure Warehousing & Inventory Management

1. Warehousing Strategy

Implementation How-To:

1. Establish a secure, climate-controlled **central staging warehouse** facility (can be vendor-provided or NYCPS facility) for initial receiving, VAT, preparation, and buffer stock storage.
2. Implement strict physical security controls for the warehouse: limited access (logged

entry/exit), secure storage cages/rooms, surveillance cameras.

3. Consider smaller, secure **regional depots or SBC-managed swap stock locations** for forward deployment of ready-to-install devices and immediate swap units, but maintain central inventory control.

Responsibility: Hardware Logistics Lead, Security Team (Physical Security Requirements), potentially Facilities Management.

2. Centralized Inventory Management System (Integrated w/ TMS)

Implementation How-To:

1. Utilize the **TMS Device Management Module** (to be built as part of the project - see Solution Design 2.8) as the single, authoritative system of record for *all* hardware assets.

2. **Mandatory Data Fields:** Serial Number (Device), MAC Address, IMEI (if cellular), Model Number, Asset Tag ID (Unique NYCPS ID), Procurement PO#, Purchase Date, Warranty

Expiration Date, Current Status (`In Stock`, `Staging`, `Ready`, `Deployed`, `In Repair`, `Awaiting Disposal`, `Lost/Stolen`, `Disposed`), Current Location (Warehouse ID, SBC Depot ID, Vehicle ID - transient), Assigned User (Driver ID - transient), Last Check-in Timestamp, OS/Firmware Version, Battery Health Status (if available), Maintenance History Log (linked repairs/RMAs).

3. **Barcode Scanning:** Implement barcode scanning (using USB scanners or mobile app) for all inventory movements (Receiving, Kitting, Distribution, Installation, Swap, RMA, Disposal) to ensure accuracy and efficiency. Inventory system *must* support barcode input.

4. **API Integration:** Ensure the TMS Device Management Module has APIs for integration with:
    - Procurement System (for PO data).
    - Ticketing System (for linking RMAs/repairs).
    - MDM System (for syncing status, OS version, potentially battery health).

- **Asset Disposal Vendor (for receiving destruction certificates).**

Tools: TMS Device Management Module (Requires Development), Barcode Scanners, Jira/Ticketing System, MDM Platform, AWS APIs.

Responsibility: Hardware Logistics Lead (Process Owner), Inventory Manager (Data Accuracy), Development Team (Building Module), DevOps (API Integrations).

3. Receiving & Inventory Intake Process

Implementation How-To:

1. **Vendor ships hardware to central staging warehouse referencing NYCPS PO number.**
2. **Warehouse staff performs physical count verification against packing slip and PO. Note any discrepancies immediately.**
3. **Perform physical inspection of packaging and sample units for shipping damage.**
4. ****Scan Serial Numbers:** Scan serial number barcode of *every* received device and peripheral into the Inventory System, marking**

status as "Received/Staging". Link to PO number.

5. Initiate Vendor Acceptance Testing (VAT) on required sample size. Update status of tested units (`VAT Passed`, `VAT Failed`).
6. Upon successful VAT for a batch, update status of all non-failed units in batch to "In Stock" or "Ready for Prep". Segregate failed units for RMA process.
7. Acknowledge receipt formally to Procurement/Finance for invoice processing *only after* successful VAT.

Responsibility: Warehouse Staff, Inventory Manager, QA Team (VAT), Procurement Liaison.

4. Buffer Stock & Reorder Management

Implementation How-To:

1. Define minimum buffer stock levels for central inventory and potentially regional/SBC swap locations based on anticipated failure rates (initial estimate based on vendor data, refine with actuals), RMA turnaround times, and rollout velocity. Buffer includes both the

contracted 5% initial spares and expected 10% annual replacement pool.

2. **Inventory system tracks stock levels against defined minimums.**
3. **Implement automated alerts or regular manual reviews to trigger re-ordering from vendor or refurbishment cycle when stock levels approach minimum thresholds.**
4. **Manage refurbishment pool separately within inventory system.**

Responsibility: Inventory Manager, Hardware Logistics Lead.

C. Stage 3: Device Preparation, Kitting & Configuration

1. Secure Device Imaging & Configuration (Standardization)

> ***Automate device configuration as much as possible using MDM or provisioning tools for consistency and efficiency at***

scale.

Implementation How-To:

1. **Develop a **Golden Image** or configuration profile for the chosen mobile device OS (Android/iOS). This *must* include:**
    - **Required OS version and security patch level.**
    - **Security hardening configurations (e.g., disabling unnecessary services/ports, enforcing screen lock, storage encryption verification).**
    - **Pre-installation of the latest approved TMS Driver Application version.**
    - **Enrollment into the chosen **Mobile Device Management (MDM)** solution (e.g., VMWare Workspace ONE, Microsoft Intune, Jamf - must support GovCloud if managing sensitive config).**

- **Configuration of device restrictions via MDM policy (e.g., prevent app installation/removal, restrict settings changes, enforce security policies).**
- **Installation of necessary root certificates for secure communication.**
- **Application whitelisting (allow only TMS app and essential system apps).**

2. **Automate the application of this Golden Image/Configuration Profile using MDM enrollment features (e.g., Android Zero-Touch Enrollment, Apple Business Manager DEP) or dedicated provisioning tools during the preparation stage.**
3. **Verify successful configuration/enrollment via MDM console and automated checks. Update device status in Inventory System to "Prepared" or "Ready for Kitting".**

Tools: MDM Platform, Android Zero-Touch/Apple Business Manager, OS Imaging/Provisioning tools (if needed), GitLab (for storing config profiles/scripts).

Responsibility: DevOps/MDM Admin, Security Team (Policy Definition), Hardware Logistics Team (Execution).

> ***Standardized, secure configurations enforced via MDM are crucial security controls.***

2. Physical Asset Tagging

Implementation How-To:

1. **Procure durable, tamper-evident asset tags with unique NYCPS identifiers and barcodes.**
2. **During preparation, affix asset tag securely to *each* mobile device and potentially major peripherals (scanners).**
3. **Scan the NYCPS asset tag barcode and associate it with the device's manufacturer serial number within the Inventory Management System.**

Responsibility: Hardware Logistics Team/Warehouse Staff.

3. Kitting Process

Implementation How-To:

1. **Define standard kit contents based on installation requirements (e.g., Prepared Device, Protective Case applied, specific Mount Type, Charger, QR Scanner, potentially pre-printed starter pack of generic QR tags/student key tags for initial distribution).**
2. **Establish dedicated kitting stations in the warehouse.**
3. **Use a checklist (physical or digital within inventory system) to ensure all required items are included in each kit.**
4. **Package kits securely for transport, clearly labeled for the target SBC/Depot and referencing devices included (via manifest or scan).**
5. **Update inventory system status for devices included in kits to "Kitted" or "Ready for Distribution".**

Responsibility: Hardware Logistics Team/Warehouse Staff.

D. Stage 4: Secure Distribution & Logistics

1. Phased Distribution Plan

Implementation How-To:

1. **Develop a detailed Distribution Schedule tightly aligned with the overall Phased Rollout Plan (Section VI of Cutover Strategy) and SBC installation schedules.**
2. **Coordinate distribution waves (delivery/pickup schedules) with SBC POCs well in advance.**

Responsibility: Hardware Logistics Lead, PM, SBC Liaisons.

2. Secure Transport & Chain of Custody

Implementation How-To:

1. **Utilize approved, bonded carriers offering trackable shipping services for deliveries to SBC depots. Require signature confirmation upon delivery.**
2. **If SBCs pick up from central staging, establish scheduled appointments and require authorized personnel identification.**

3. Maintain strict **Chain of Custody** documentation for all movements:
    - Log includes: Date/Time, From Location, To Location, Carrier/Tracking # (if shipped) or Pickup Person Name/ID, List/Manifest of Serial Numbers Transferred, Signatures of Sending/Receiving parties.
    - Update Inventory System location field immediately upon transfer/receipt confirmation.

Responsibility: Hardware Logistics Lead, Warehouse Staff, SBC POCs (Receipt Confirmation).

> **Loss or theft during transit is a significant risk. Secure transport and chain of custody are critical.**

3. SBC Receipt & Verification

Implementation How-To:

1. SBC POC receives shipment/pickup. Performs immediate physical count verification against

shipping manifest. Reports discrepancies *immediately* to Hardware Logistics Lead.

2. SBC POC scans received device serial numbers to confirm receipt within the Inventory Management System (potentially via a simple web portal or app provided for SBCs).
3. SBC POC formally acknowledges receipt (digital signature or signed manifest returned).
4. Devices moved to secure storage location at SBC depot. Status updated to "Received at SBC".

Responsibility: SBC POC, Hardware Logistics Lead (Monitoring/Reconciliation).

E. Stage 5: Installation, Verification & Activation

1. Installation Process & Scheduling

Implementation How-To:

1. **Responsibility Clarification: Formally document whether installation (mounts, power, peripherals) is performed by Vendor Field Techs, dedicated Installation Team, or trained SBC Mechanics (as per contract/SOW).**

2. **Develop detailed, vehicle-type-specific **Installation Standard Operating Procedures (SOPs)** covering: Mount placement (driver view, passenger safety, scanner access), secure mounting techniques, power connection method (fuse tap vs direct wire - ensuring no battery drain, follow OEM guidelines), cable routing/management, peripheral connection, adherence to NYDMV regulations. SOPs include photos/diagrams.**

3. **Use a Ticketing System (Jira SM or other) integrated with the Inventory System to schedule and track installation appointments per vehicle.**

4. **Field Tech Coordinator works with SBC POCs to schedule installations efficiently, minimizing bus operational downtime (targeting off-hours, weekends, non-school days where possible).**

Responsibility: Field Tech Coordinator, Installation Team Lead/Vendor, SBC POCs.

2. Installation Execution & Verification Checklist

Implementation How-To:

1. Installer follows the documented SOP for the specific vehicle type.
2. Installer completes a mandatory **Installation Checklist** (digital via app preferred, or paper) for *each* vehicle install. Checklist includes:
    - Vehicle ID, Date/Time, Installer Name/ID.
    - Device Serial Number(s) Installed (scanned).
    - Mount Securely Installed & Positioned Correctly (Photo verification optional).
    - Power Connection Verified (Device powers on with ignition, off when appropriate, no parasitic drain).
    - Cabling Secured & Routed Safely.

- **Peripheral(s) Connected & Tested (e.g., QR scanner successful scan).**
- **Device Boot-up & TMS App Launch Verified.**
- **Initial GPS Lock Acquired Verified.**
- **Connectivity Check (Cellular/Wi-Fi signal strength).**
- **Installer Signature, SBC Representative Signature (confirming work completion/vehicle condition).**

3. **Completed checklist submitted/scanned and linked to the Installation Ticket and Inventory Record.**

Responsibility: Installer (Execution/Checklist), SBC Rep (Sign-off), Field Tech Coordinator (Tracking).

Quality Gate: Successful completion and sign-off of Installation Checklist required for each device deployment.

3. System Activation & Inventory Update

Implementation How-To:

1. **Upon successful installation verification (checklist received/processed):**
    - **Update device status in Inventory System to **"Deployed/Active"**.**
    - **Associate device serial number with the specific Vehicle ID in the Inventory System.**
    - **(If MDM used) Verify device checks into MDM server and receives production policies.**
2. **The TMS system uses the Driver Login process (associating Driver ID + Device ID + Selected Route/Vehicle ID for the shift) to link the specific device to operational activity.**

Responsibility: Inventory Manager/Automated Process, MDM Admin, TMS Application Logic.

F. Stage 6: Ongoing Maintenance & Lifecycle Management

1. Firmware/OS Update Strategy (Mandatory)

> ***Maintaining up-to-date OS/Firmware is critical for security compliance and stability.***

Implementation How-To:

1. **Vendor Notification:** Hardware/OS vendor *must* provide proactive notification of upcoming critical security patches or major OS updates relevant to the deployed devices.
2. **Testing:** Security/DevOps/QA teams obtain update packages and rigorously test them on a representative sample of devices in a non-production environment. Validate TMS Driver App compatibility, performance, battery life impact, and core functionality.
3. **Rollout Planning:** Plan phased rollouts for approved updates using the **MDM platform**. Target off-peak hours (e.g., overnight) to minimize disruption. Define waves (e.g., pilot group -> broader SBCs -> full fleet).
4. **Deployment via MDM:** Use MDM capabilities to schedule and push updates

remotely to devices over-the-air (OTA). Monitor deployment status via MDM console.

5. **Rollback Plan:** Maintain procedures for halting rollout or potentially rolling back devices (if supported by MDM/OS) in case of widespread issues post-update.

6. **Documentation:** Track deployed OS/Firmware versions per device in the Inventory System (synced from MDM). Document update testing and rollout history.

Responsibility: DevOps/MDM Admin (Execution), Security Team (Patch Assessment/Approval), QA Team (Testing), Hardware Logistics Lead (Coordination).

2. Battery Health Management

Implementation How-To:

1. **Monitoring (If Feasible):** If the chosen device and MDM solution support reliable battery health reporting (e.g., cycle count, maximum capacity %), configure MDM to collect this data periodically. Integrate data into Inventory System. Set thresholds/alerts for devices showing significant degradation (e.g., <80% original capacity).

2. **Monitoring (Age/Usage Based):** If direct health reporting is unreliable, track device age and potentially usage patterns (via TMS logs) as proxies. Establish expected lifespan (e.g., 3 years) and proactively flag devices nearing end-of-life for potential replacement.

3. **Proactive Replacement:** Schedule proactive replacement of devices identified via monitoring *before* they cause operational failures due to poor battery life. Integrate replacement into the standard RMA/Swap Stock process.

4. **Track Replacements:** Log all battery-related replacements specifically in the Inventory System maintenance history. Analyze trends to refine lifespan estimates.

Responsibility: Hardware Logistics Lead, Inventory Manager, MDM Admin, SRE/Ops (Monitoring Integration).

3. Device Status Monitoring (Operational)

Implementation How-To:

1. TMS Driver App *must* report key device status metrics (Battery Level %, Connectivity

Status - Cellular/WiFi, GPS Signal Quality) periodically to the TMS backend.

2. **MDM platform (if used) provides additional status (Online/Offline, Last Check-in, Policy Compliance).**
3. **Integrate critical status data into the **OPT Administrative Console** and potentially the **SBC Admin Console** for operational visibility.**
4. **Configure **CloudWatch Alarms** based on aggregated device status data (e.g., % of devices offline > threshold, % of devices with battery < 20% during shift hours). Alerts routed to SRE/Ops and potentially SBC Liaisons/Support.**

Responsibility: Mobile Dev Team (App Reporting), SRE/Ops (Monitoring/Alerting), DevOps/MDM Admin (MDM Integration).

G. Stage 7: Swap Stock / Break-Fix / RMA Process (Detailed Flow)

Implementation How-To:

1. **Maintain Local Swap Stock:** Hardware Logistics Lead ensures each designated SBC depot/location maintains the agreed minimum level of *fully prepared* (imaged, configured, kitted) swap devices based on fleet size and failure trends. Inventory System reflects "Swap Stock" location.

2. **Step 1: Fault Detected & Reported:** Driver/Attendant experiences device issue (won't turn on, app crash, scanner fail, physical damage). Driver *must* report immediately to their SBC Dispatcher.

3. **Step 2: Initial SBC Troubleshooting:** Dispatcher attempts basic troubleshooting (reboot, check power) per provided guide (QRG/KB).

4. **Step 3: Issue Ticket Creation:** If basic troubleshooting fails, SBC Dispatcher (or Driver via app if functional) *must* create a support ticket in the designated system (NYCPS system integrated with vendor system), detailing the Device Serial Number, Vehicle ID, Driver ID, and specific problem description. Ticket routes to L1/Hardware Support Queue.

5. **Step 4: Swap Device Authorization:** L1/L2 support reviews ticket. If issue indicates likely hardware failure or cannot be resolved

remotely, they authorize a swap and notify SBC Dispatcher via ticket update/communication channel.

6. **Step 5: Execute Swap at Depot:** SBC Dispatcher issues a replacement device from local swap stock to the Driver. Driver logs into new device. SBC Dispatcher securely stores the faulty device.

7. **Step 6: Inventory System Update (Critical):** SBC Dispatcher (or automated process triggered by Driver login on new device if feasible) *must* update the Inventory System immediately:
    - Mark faulty device (by serial #) status as "Awaiting RMA Pickup", location = SBC Depot X.
    - Mark replacement device status as "Deployed/Active", location = Vehicle ID Y, assigned user = Driver ID Z.

8. **Step 7: Faulty Device Collection & Shipment:** Periodically (e.g., weekly), Hardware Logistics Coordinator arranges secure pickup or provides prepaid shipping labels for SBCs to return collected faulty devices (batched) to the central repair

depot/vendor facility. Chain of Custody maintained. Inventory status updated to "In Transit to Repair".

9. **Step 8: RMA Processing (Vendor/Depot):**
    - Repair Depot receives devices, updates Inventory status to "In Repair".
    - Technician diagnoses issue, links to original ticket. Determines Warranty vs. Non-Warranty Damage.
    - **If Warranty:** Repair or replace device. Perform QA checks. Update Inventory status to "Refurbished/Ready" or "Replaced".
    - **If Non-Warranty Damage:** Document damage cause (photo evidence). Follow defined process for notifying NYCPS PM/Finance/SBC regarding potential chargeback or use of buffer stock. If repaired, update status; if scrapped, update status to "Awaiting Disposal".

10. **Step 9: Replenish Swap Stock:** Refurbished/replaced devices are re-imaged/prepared (Step C) and shipped back to replenish central inventory or directly to SBC swap stock locations based on need. Inventory status updated ("In Stock at SBC Depot X").

11. **Step 10: SLA Monitoring & Escalation:** Hardware Logistics Lead monitors RMA ticket aging and vendor turnaround times against contractual SLAs using reports from the integrated ticketing/inventory system. Escalate delays via Vendor Manager per defined process.

Responsibility: Driver (Reporting), SBC Dispatcher (Initial Triage, Swap Execution, Inventory Update), L1/L2 Support (Authorization), Hardware Logistics Lead (Coordination, Monitoring, Escalation), Repair Vendor/Technicians (Diagnosis/Repair), Inventory Manager (System Accuracy).

> **Failure to accurately track device swaps and RMAs in the inventory system leads to lost assets and inaccurate status reporting. Timely swap stock replenishment is crucial for driver uptime.**

H. Stage 8: Lost/Stolen Device Procedure (Mandatory & Urgent)

Implementation How-To:

1. **Immediate Reporting:** Driver/SBC *must* report a suspected lost or stolen device *immediately* (within minutes/hours) via a dedicated high-priority channel (e.g., specific support hotline, critical ticket type). Report must include last known location/time, device serial #, user.
2. **Remote Lock/Wipe Execution (Urgent):** Security Team / MDM Admin *must* immediately (within 1 hour of report) trigger remote lock and/or full data wipe command via the MDM platform. **Verification of command execution is critical.**
3. **Incident Logging:** Log the event in the security incident tracker and the device Inventory System, marking status as "Lost/Stolen".
4. **Access Review:** Security team reviews recent access logs for the device/user account for any suspicious activity prior to loss.
5. **Replacement:** Issue replacement device via standard swap process.

6. **Formal Reporting:** Follow established NYCPS procedures for reporting lost/stolen assets, potentially involving investigations or police reports depending on circumstances and policy.

Responsibility: Driver/SBC (Immediate Reporting), Security Team/MDM Admin (Immediate Lock/Wipe), Inventory Manager (Status Update), PM/NYCPS Security Office (Formal Reporting/Investigation).

Rapid response, remote wipe capability, and formal reporting are crucial for mitigating data privacy risks (FERPA/2-d) associated with lost/stolen devices containing PII.

I. Stage 9: End-of-Life Management & Secure Disposal (Certified)

Implementation How-To:

1. **EoL Identification:** Logistics Lead/Inventory Manager generates quarterly reports from Inventory System identifying devices exceeding defined lifespan (e.g., 5

years), warranty expiration, or marked as irreparable (non-warranty).

2. **Replacement Planning:** Integrate EoL projections into hardware forecasting and buffer stock management to plan for replacements.**

3. **Device Collection:** Coordinate systematic collection of EoL devices from SBC depots (e.g., during swap replenishment deliveries, scheduled pickups). Update Inventory status to "Awaiting Disposal". Store collected devices securely at central staging.**

4. **Secure Data Destruction (Mandatory & Verifiable):**

    - **Execute MDM remote wipe command *again* as a first step on collected devices.**

    - **Perform secondary data sanitization using approved software tools meeting NIST 800-88 "Purge" or "Clear" standards on *every* device. Log successful sanitization per serial number.**

- **For devices that fail software sanitization or per NYCPS policy for highly sensitive data, *physical destruction* (shredding/disintegration) via a certified e-waste vendor is mandatory.**

5. **Engage Certified E-Waste Vendor:** Contract with a reputable, certified e-waste disposal vendor adhering to R2, e-Stewards, or equivalent standards and all environmental regulations. Vendor *must* provide auditable chain of custody and **formal Certificates of Destruction** for both data sanitization (if performed by them) and physical disposal.

6. **Inventory Reconciliation:** Update Inventory System status to "Disposed/Destroyed" *only after* receiving the signed Certificate of Destruction. Link certificate to inventory records.

7. **Record Retention:** Securely archive Certificates of Destruction and associated inventory logs for audit purposes (minimum 7 years or per NYCPS policy).

Responsibility: Hardware Logistics Lead (Process Owner), Inventory Manager (Tracking), Security Team (Defining

Destruction Standards), Compliance Officer (Verifying Certs), Certified E-waste Vendor (Execution/Certification), Procurement (Vendor Contract).

> ***Improper disposal of devices containing PII is a major compliance violation. Certified destruction and documentation are non-negotiable.***

J. Stage 10: Auditing, Reporting & Continuous Improvement

Implementation How-To:

1. **Regular Inventory Audits:** Conduct quarterly physical spot checks at central warehouse and selected SBC depots, reconciling physical counts against Inventory System records. Investigate and resolve discrepancies immediately.
2. **Process Audits:** Periodically (e.g., semi-annually) audit adherence to key processes (Receiving, Kitting, Installation Checklist Completion, Swap/RMA workflow, Disposal

procedures) via documentation review and interviews.

3. ****KPI Reporting:** Logistics Lead generates and reviews monthly reports (derived from Inventory/Ticketing system data) covering:**
    - **Inventory Levels (Total, Per Location, Swap Stock vs. Target)**
    - **Device Status Distribution (% Active, In Repair, Lost/Stolen, etc.)**
    - **RMA Turnaround Time (Avg, Max vs. SLA)**
    - **Device Failure Rates (by Model, Age, SBC - identifying trends)**
    - **Installation Success Rate & Timeliness**
    - **EoL Projections vs. Budget**
    - **Disposal Certification Status**
4. ****Review & Improvement:** Discuss KPIs and audit findings in Monthly FinOps/Ops Reviews and MBRs. Identify areas for process improvement, automation, vendor performance management, or potential hardware**

specification changes. Update relevant strategy/process documents based on lessons learned.

Responsibility: Hardware Logistics Lead, Inventory Manager, Internal Audit (if applicable), PMs, Vendor Manager.

IX. Conclusion: Ensuring Physical Asset Integrity & Operational Readiness

This Prescriptive Hardware Lifecycle & Logistics Management Strategy provides the exhaustive framework necessary to manage the complex physical infrastructure underpinning the NYCPS TMS. By implementing these detailed, mandatory processes for procurement, acceptance testing, secure inventory management, standardized preparation, controlled distribution, verified installation, proactive maintenance (firmware/battery), efficient break-fix/RMA handling, rigorous lost/stolen procedures, and certified secure disposal, we establish robust control and accountability over ~11,000+ critical assets dispersed across NYC.

The emphasis on automation (inventory tracking, MDM, monitoring), clear roles, integration with support ticketing and project governance, data-driven performance monitoring (KPIs/SLAs), and continuous

auditing ensures efficiency, minimizes operational disruption, mitigates security and financial risks associated with hardware loss or failure, and guarantees compliance with all asset management and data destruction requirements. Strict adherence to this plan is critical for the successful deployment, sustained operation, and overall integrity of the TMS.