

TECHNOLOGICAL OBSOLESCENCE



FLEET & DEPOT OPERATIONS PROTOCOL



Trigger Points

- OEM announces end-of-life for hardware/software.
- Discontinued support or security patches.
- Spare parts unavailable or incompatible.



Responsibility

Depot Manager

Control Room

Fleet Controller

IT Security/ Head

A. DETECTION & REPORTING



Responsibility:

Depot Staff

IT Support Personnel

- 🔍 Identify obsolete systems or unsupported components.
- 📞 Report to Depot Manager, Fleet Controller, IT Security Lead.
- 🚫 Do not attempt manual software updates or unauthorized fixes.

B. ASSESS & ISOLATE



Responsibility:

Depot Manager

IT Support Personnel

- 📋 Check affected buses, chargers, and IT systems.
- 🚫 Disconnect unsupported hardware/software from network.
- 🔒 Disable remote features without security patches.

C. MAINTAIN OPERATIONS



Responsibility:

Depot Manager

Fleet Controller

- 🚌 Switch to manual charging and dispatch.
- 📄 Use printed route plans and offline logs.
- 📞 Communicate with drivers via secure channels.

D. COORDINATE & UPGRADE



Responsibility:

CONTROL ROOM

OEM Technical Support

- 🏢 Contact OEM for migration roadmap, firmware updates, retrofit kits.
- 📄 Negotiate service continuity agreements.

E. EMERGENCY ACTIONS - SOPS



Responsibility:

Depot Manager

SOPs for Depot Manager during technology failure incident

- Maintain inventory audit of obsolete parts and systems.
- Isolate unsupported chargers or hardware from active network.
- Implement manual scheduling, route management, charging and dispatch if smart systems fail.
- Document all operational changes for compliance.



Responsibility:

Fleet Controller

SOPs Fleet Controller technology failure incident

- Identify buses with outdated BMS or telematics.
- Disable remote features if security patches are unavailable.
- Switch to manual route planning and driver communication.
- Log trips offline until systems are upgraded..



Responsibility:

IT Security/ Head

SOPs for IT Head/ security during Technological Obsolescence

- Validate software versions and patch status.
- Disconnect unsupported systems from network to prevent cyber risk.
- Activate backup servers for fleet data.
- Notify CERT-In if vulnerabilities arise due to obsolescence..



Responsibility:

OEM Technical Support

SOPs for OEM Technical Support during cyber threat/ attack

- Request migration roadmap for hardware/software upgrades.
- Secure firmware updates or retrofit kits.
- Negotiate service continuity agreements for critical systems.