



FLEET & DEPOT OPERATIONS PROTOCOL



Trigger Points

- Unusual system behavior, unauthorized access, data anomalies, or alerts from cybersecurity tools.

A. DETECTION & IMMEDIATE REPORTING



Responsibility: IT support Fleet Operator Depot Supervisor

- On identification of trigger, immediately report the incident to the Depot Control Room and IT Security Lead.
- Record the time, nature, and source of the anomaly.
- Avoid interacting further with the affected system.

B. ISOLATION & CONTAINMENT



Responsibility: IT Security / Head

- Disconnect affected systems, disable remote access, freeze changes.
- Preserve logs for investigation.
- Notify staff to avoid affected systems.

C. RESPONSE ACTIVATION & MANUAL OPERATIONS



Responsibility: IT Head Depot Manager Fleet Controller

Activate Cyber Incident Response Team (CIRT) - Assign roles for investigation, containment, and recovery.

- Switch to manual dispatch and route monitoring.
- Monitor charging manually and coordinate with drivers via secure channels.
- Maintain service continuity using offline tools.

D. EXTERNAL NOTIFICATION & RECOVERY



Responsibility: IT Head Legal Officer OEM Support

- Inform OEM, cybersecurity partners, and transport authorities.
- Notify **CERT-In** or regulators if data breach is suspected.
- Conduct forensic investigation and identify vulnerabilities.
- Patch systems and restore operations securely.
- Validate system integrity before reconnecting to the network.

*Computer Emergency Response Team – India (CERT-In) - is the national nodal agency for cybersecurity incidents under the Ministry of Electronics and Information Technology (MeitY), Government of India.



Responsibility

IT Security / Head

IT support

Depot Manager/ Fleet

OEM Technical Support

D. EMERGENCY ACTIONS - SOPS



Responsibility:

Depot Manager

SOPs for Depot Manager/ Fleet Controller during Cyber Threat/ attack

- Acknowledge cyber incident and inform IT Security Lead.
- Secure depot systems and disconnect affected chargers, terminals, or buses.
- Switch to manual operations for charging and dispatch.
- Coordinate with drivers using radio/phone for route instructions.
- Use printed or verbal route plans for dispatch & Track buses manually and log trip and charging data offline.
- Support IT and OEM teams during investigation and recovery.



Responsibility:

IT Security

SOPs for IT Head/ security during Cyber Threat/ attack

- Validate threat and isolate affected systems.
- Disable remote access and save logs.
- Disconnect compromised buses/systems from network.
- Activate backup servers and manual controls.
- Run diagnostics to find breach source.
- Update Depot Manager and Control Room.
- Activate CIRT and block suspicious IPs/accounts.
- Notify CERT-In and OEM if breach confirmed.
- Lead recovery and patch systems.



Responsibility:

OEM Technical Support

SOPs for OEM Technical Support during cyber threat/ attack

- Diagnose vehicle systems (e.g., BMS, telematics).
- Provide firmware patches or resets.
- Validate systems before reintegration.
- Support forensic analysis if needed.