Service Level Agreement (SLA)
IT Support to SMSA Service Centers

Completed and agreed by Central IT and the Service Center.

Provider: Central IT, [Kashan Khalid, National IT Manager]
Customer: SMSA Service Centers, [Madhu Kalayathinal, Head of Service Centers]
Effective date: [6 July 2026] · **Review cycle:** [monthly] Version: 1.0

1. Purpose and scope

Central IT provides technology support to the Service Center outlets. This SLA defines the service, the service levels, and the responsibilities of each side.

- **In scope:** outlet endpoints and POS devices, network connectivity including Telephone, internet and mobile SIM new request/transfer/ cancellations, user/IT support, email & VPN support, CORE support, TAS biometric support, Digital TV support, all kind of hardware support, incident response including site visits when required, access provisioning and revocation, patching and security. inventory maintenance of the IT assets record and new and replacement requirement submissions.
- **Out of scope:** [None]

2. Service hours and coverage

- **Support hours:** outlet operating hours / business hours / 24x7
- **Coverage:** all KSA regions, CR / WR / ER / SR / NR and SSC projects and events.

3. Service levels (targets agreed)

Priority	Definition	Response target	Resolution target
P1, Critical	Outlet / POS down, no service	15 minutes	4 Hours
P2, High	Degraded service, single device/user down	1 hour	1 Business Day or 8 business hours
P3, Normal	Routine request or minor issue	4 business hours	2 Business days
P4, Service Request (Optional)	New device, access, standard change	1 Business Day	3 Business days

- **System / network availability target:** 99.0%, measured over outlet operating hours.

4. Responsibilities

Central IT (provider)	Service Center (customer)
Provision and revoke access; hold admin rights	**Set business requirements and priorities**
Support endpoints, POS, and network	**Set and hold IT to the service levels**
Respond and resolve to the targets above	Report incidents accurately and promptly
Security, patching, monitoring	Provide access for support; nominate a point of contact
Report on service performance	Attend the service review

Kashan 06 July 26

06/07/26

5. Escalation path

A. Service escalation (a missed target, an unresolved incident):

- **Operational:** L1 [service desk] → L2 [IT support lead] → L3 [Kashan, IT]
- **Business:** [Service Center point of contact] → L1 [SSC Regional Manager] → L2 [Madhu]
- **Unresolved between IT and the Service Center:** referred to the **Office of the CHRO** (or the designated IT-governance forum) for a decision.

B. Control or security breach (access misuse, a bypass, a policy or security violation surfaced through the service): referred to **Internal Audit/QRM / the CAE** under the Company's assurance policy. This is an independent-assurance referral, kept **separate** from service escalation, Internal Audit is not part of the service-escalation chain.

6. Reporting and review

- **Monthly service report:** tickets raised/closed, mean time to resolve, SLA-compliance %, notable incidents.
- **Service review meeting:** [monthly], Central IT and the Service Center, to review performance and priorities.

7. Change and exceptions

Any change to scope or service levels is agreed in writing between Central IT and the Service Center and recorded as a new version of this SLA.

8. Sign-off

	Name	Signature	Date
Central IT	Kashan Khalid		06th July 2026.
Service Center	Madhu Kalayathinal		06/07/26
CHRO	Dr Ziyad Alghannam		07/07/26

**Framework issued by the Office of the CHRO. Targets, hours, and escalation are completed and agreed by Central IT and the Service Center. **