MONTHLY SERVICE REPORT · REMOTE PLAN

Syarikat Contoh Sdn Bhd

Reporting period 1 to 31 October 2026 · fictional company, mock data

PLAN	SITES	MONITORED	PREPARED BY
Remote 24x7	2 (HQ, Branch)	62 devices	Nur Aisyah K.

AVAILABILITY	SLA KPIS MET	INCIDENTS	P1 INCIDENTS
99.97%	6 / 6	21	0

SAMPLE

Summary

- Critical services were available **99.97%** of the month, against a target of 99.5%. The largest loss was 40 minutes on the HQ backup link (Maxis).
- 21 incidents: **0 × P1, 4 × P2, 11 × P3, 6 × P4**. All four P2s were acknowledged within the 30-minute target; the median was 5 minutes.
- **Action needed:** SRV-FILE-01 drive D: reached 84% and, at the current rate, will be full by mid-January 2027. See recommendation 1.

SLA scorecard

KPI	TARGET	RESULT	STATUS
P1/P2 alerts acknowledged within target	≥ 95%	100% (4 of 4)	Met
Monitoring platform availability	≥ 99.5%	99.98%	Met
Coverage register accuracy (10 sampled)	≥ 98%	100%	Met
Shift handover logs completed	100%	93 of 93	Met
Monthly report delivered	Working day 5	06 Nov (day 5)	Met
Escalation matrix call-tested	Monthly	21 Oct	Met

Service credits this month: none. Response times are measured from the first alert to acknowledgement by a Dunia Canggih engineer.

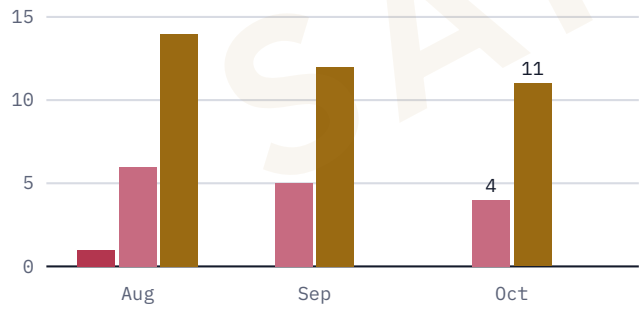
Availability by service

October has 44,640 minutes

SERVICE	SITE	DOWNTIME	AVAILABILITY
Internet, primary (TM 500 Mbps)	HQ	9 min	99.98%
Internet, backup (Maxis 100 Mbps)	HQ	40 min	99.91%
Internet (TM 100 Mbps)	Branch	0 min	100.00%
Site-to-site VPN	HQ ↔ Branch	22 min	99.95%
ERP portal	HQ	13 min	99.97%
Email gateway	HQ	0 min	100.00%
File server SRV-FILE-01	HQ	0 min	100.00%
Core switch SW-HQ-CORE-01	HQ	0 min	100.00%
Critical services, weighted			**99.97%**

Incidents by priority

last 3 months



P1 P2 P3 P4 not shown (6 in October).

Response times

October

PRIORITY	COUNT	MEDIAN ACK	TARGET
P1	0	–	15 min
P2	4	5 min	30 min
P3	11	14 min	2 hrs
P4	6	3 hrs	1 day

P2 incidents

DATE	INCIDENT	ACK	RESOLVED BY	DURATION
04 Oct 21:12	HQ backup link down; firewall stayed on primary, no user impact	4 min	Maxis	40 min
11 Oct 10:37	Site-to-site VPN dropped; Branch could not reach ERP	3 min	Client IT	22 min
19 Oct 15:02	ERP portal response 3.4 s, then unreachable	6 min	ERP vendor	13 min
27 Oct 08:51	SRV-SQL-01 memory 96% for 20 min	7 min	Client IT	48 min

SAMPLE

Resolver and vendor performance

time from our escalation to service restored

RESOLVER	TICKETS	AVERAGE RESTORE	THEIR SLA	STATUS
TM (ISP, HQ and Branch)	1	9 min	4 hrs	Met
Maxis (ISP, HQ backup)	2	5 hrs 10 min	4 hrs	Missed
Client IT team	14	1 hr 25 min	–	–
ERP vendor	1	13 min	2 hrs	Met

Maxis missed its 4-hour restore target on one of two tickets (MX-439120, packet loss, 9 hrs 40 min). You may be able to claim a rebate under your Maxis contract.

Capacity watch

readings at 31 Oct

ITEM	NOW	30 DAYS AGO	FORECAST
SRV-FILE-01 drive D: (2 TB)	84%	79%	Full around 15 Jan 2027
SRV-SQL-01 drive E: (1 TB)	74%	72%	Above 85% around May 2027
HQ primary link, monthly peak	71%	66%	Watch; alert line is 80%
UPS-HQ-01 load	42%	41%	Stable

Coverage changes

Added: SW-HQ-L3-05 (new floor switch), UPS-ALG-02 (Branch UPS).
Removed: SRV-OLD-PRN-01 (retired print server).

Total monitored at month end: 62 devices (12 over the 50 included, billed as one block of 25).

Escalation matrix check

All 9 contacts call-tested on 21 Oct. One change: client IT on-call mobile number updated.

Next check: November 2026.

Requests outside the Remote plan

DATE	REQUEST	WHAT WE DID
08 Oct	Open a firewall port for a new supplier portal	Referred to client IT. Configuration changes are covered by the L2 add-on.
23 Oct	Staff laptop cannot print	Referred to your IT helpdesk. End-user support is not part of the NOC service.

Recommendations

#	RECOMMENDATION	OWNER	BY
1	Extend SRV-FILE-01 drive D: or archive files older than 3 years	Client IT	31 Dec 2026
2	Raise the repeated Maxis backup-link faults with your Maxis account manager	Client IT Manager	30 Nov 2026
3	Renew the SSL certificate for portal.contoh.example (expires 29 Nov 2026)	Client IT	22 Nov 2026

SAMPLE

Appendix A · Monitoring coverage register extract, 15 of 62 entries

DEVICE	TYPE	IP	SITE	CRITICALITY	METHOD
FW-HQ-01	Firewall	10.10.0.1	HQ	Critical	ICMP, SNMP v3
FW-ALG-01	Firewall	10.20.0.1	Branch	Critical	ICMP, SNMP v3
SW-HQ-CORE-01	Core switch	10.10.0.2	HQ	Critical	ICMP, SNMP v3, syslog
SW-HQ-L3-05	Access switch	10.10.0.15	HQ	High	ICMP, SNMP v3
WAN-HQ-TM	Internet link	203.0.113.10	HQ	Critical	ICMP, SNMP (edge)
WAN-HQ-MAXIS	Internet link	198.51.100.22	HQ	High	ICMP, SNMP (edge)
CPE-HQ-TM	ISP router	203.0.113.9	HQ	High	ICMP only (ISP-managed)
SRV-FILE-01	Windows server	10.10.1.20	HQ	Critical	Agent
SRV-SQL-01	Windows server	10.10.1.21	HQ	Critical	Agent
SRV-APP-02	Linux server	10.10.1.32	HQ	High	Agent
erp.contoh.example	Web app	–	Cloud	Critical	HTTPS check, SSL expiry
portal.contoh.example	Web app	–	Cloud	High	HTTPS check, SSL expiry
WLC-HQ-01	Wireless controller	10.10.0.40	HQ	High	SNMP v2c (read-only)
UPS-HQ-01	UPS	10.10.0.60	HQ	High	SNMP v2c (read-only)
UPS-ALG-02	UPS	10.20.0.60	Branch	Medium	SNMP v2c (read-only)

The full register is attached as a separate locked PDF each month. CPE-HQ-TM is ping-only because the ISP manages the router and has not granted SNMP access.

Appendix B · Definitions

P1	Outage affecting a whole site or a critical service. Acknowledge 15 min, escalate 30 min, update every 30 min.
P2	Degraded service, or a critical component down with redundancy holding. Acknowledge 30 min.
P3	Non-critical component affected, workaround exists. Acknowledge 2 hrs.
P4	Informational or request. Acknowledge next business day.

Prepared by
Nur Aisyah K., NOC Lead
05 Nov 2026

Reviewed by
Hafiz R., Service Delivery Manager
06 Nov 2026

Issued as a locked PDF. Editing is disabled; printing and copying text are allowed. Only the copy issued by Dunia Canggih NOC with the reference above is valid. This sample uses a fictional company, fictional people and mock data.

SAMPLE