P1

PRIORITY 1 · MAJOR INCIDENT

Whole-site outage at HQ. Highest severity: acknowledge 15 min, escalate 30 min, updates every 30 min.

MAJOR INCIDENT REPORT

HQ primary internet link down

Syarikat Contoh Sdn Bhd · Tuesday 03 November 2026 · fictional company, mock data

SAMPLE

STARTED	FULL OUTAGE	LINK DOWN	CLOSED
14:06 MYT	13 min	47 min	15:10 MYT

What happened

The HQ primary internet link (TM, 500 Mbps) went down at 14:06 when a third party damaged TM's fibre during roadworks. The firewall should have switched to the Maxis backup link automatically but did not, so HQ had no internet for 13 minutes until client IT switched over by hand at 14:19. HQ then ran on the backup link, more slowly, until TM restored the fibre at 14:53.

Impact

About 120 HQ staff lost internet and cloud applications for 13 minutes, then had slower service for 34 minutes. The ERP portal was unreachable from HQ for 13 minutes. The Branch kept its own internet but lost the VPN to HQ for the same 13 minutes.

Our response against the SLA

Acknowledged	2 min	≤ 15 min
Escalated to resolver	5 min	≤ 30 min
Updates sent	every 30 min	Met

P1 · MAJOR INCIDENT · HQ PRIMARY INTERNET LINK DOWN

Timeline

all times MYT, from monitoring and call records

TIME	EVENT	BY
14:06:12	Alert: WAN-HQ-TM 100% packet loss; FW-HQ-01 wan1 down. HQ unreachable from our hub.	Monitoring
14:06:51	AI Grouped 14 related alerts into one incident. Logged in read-only to FW-HQ-01 and ran 5 approved checks (session AIS-20261103-0042).	AI assistant
14:07:24	AI Findings posted to the incident. Top suggested cause: upstream link failure, firewall failover not triggered.	AI assistant
14:08	Alert acknowledged. Declared P1 (whole site affected). Runbook RB-CONTOH-004 started.	DC hub
14:09	Tested the AI's top suggestion: Maxis backup link up, firewall still routing to wan1. Confirmed.	DC hub
14:11	Called client IT on-call (answered first ring). Asked for manual failover, runbook step 3.	DC hub
14:14	Fault logged with TM, ticket TM-1-88213457, circuit ID on file.	DC hub
14:19	Client IT switched the default route to the backup link. HQ internet restored at reduced speed.	Client IT
14:20	Update 1 emailed to the distribution list.	DC hub
14:38	TM confirmed a fibre cut caused by third-party excavation; crew on site.	TM
14:50	Update 2 emailed.	DC hub
14:53	Primary link back up after a temporary splice. Watched for 10 minutes.	TM / DC
15:05	Client IT moved traffic back to the primary link.	Client IT
15:10	Incident closed after client IT confirmed normal service. Final update emailed.	DC NOC Lead

SAMPLE

P1 · MAJOR INCIDENT · HQ PRIMARY INTERNET LINK DOWN

AI-assisted investigation suggestions reviewed by the NOC Lead

AI **Alert grouping.** 14 alerts in 40 seconds were grouped into this incident: WAN-HQ-TM loss, FW-HQ-01 wan1 down, HQ ↔ Branch VPN down, ERP HTTPS check failed from HQ, and 10 dependent checks behind the HQ firewall.

AI **What changed first.** wan1 carrier state dropped at 14:06:09, three seconds before the first ping alert. The TM router (CPE-HQ-TM) kept answering ping throughout. No configuration change on FW-HQ-01 in the previous 30 days.

Read-only checks run by AI

Session AIS-20261103-0042 · device FW-HQ-01 · account noc-ro (read-only) · run from collector COL-HQ-01 · 14:06:58 to 14:07:20 · 5 approved commands, 0 refused

TIME	CHECK	RESULT
14:06:58	Interface status, wan1	Link down; carrier lost at 14:06:09
14:07:03	Link health check status	Probe target 203.0.113.9 (TM router) **alive**, so failover was not triggered
14:07:08	Routing table, default route	Still via wan1 (primary); wan2 route standing by
14:07:14	Ping 1.1.1.1 via wan2	0% loss, 29 ms, so the backup link works
14:07:20	Device log, last 15 minutes	wan1 link-down event at 14:06:09; no config changes; no hardware errors

Ranked causes

RANK	SUGGESTED CAUSE	EVIDENCE	AI CONFIDENCE	ENGINEER FINDING
1	ISP fault beyond the TM router	Carrier lost on wan1 while the TM router stayed reachable	High	**Confirmed by TM at 14:38**
2	Firewall failover check pointing at the wrong target	AI check at 14:07:03: probe target is the TM router, which never stopped answering	High	**Confirmed in config**
3	Firewall hardware fault	Interface errors were zero before the event	Low	Ruled out

AI suggestions come from monitoring data and the read-only checks above. The AI made no changes to any device. The engineer findings and the cause on the next page are the NOC Lead's conclusions.

SAMPLE

P1 · MAJOR INCIDENT · HQ PRIMARY INTERNET LINK DOWN

Cause

Link failure: TM's fibre was cut by third-party roadworks. TM made a temporary splice on the day and scheduled a permanent repair for the night of 05 November.

Failover failure: the firewall decides whether the primary link is healthy by pinging one target, the TM router on your premises. That router stayed powered and answered, so the firewall believed the link was fine. This is why HQ went fully offline instead of moving to the backup link.

Follow-up actions

#	ACTION	OWNER	DUE	STATUS
A1	Point the firewall's link health check at two outside targets (for example 1.1.1.1 and 8.8.8.8) instead of the TM router	Client IT	10 Nov 2026	Open
A2	Add an alert when the firewall is on the primary link but the primary link cannot reach the internet	Dunia Canggih NOC	07 Nov 2026	Open
A3	Test failover during the next maintenance window, with our hub watching	Client IT + DC	14 Nov 2026	Scheduled
A4	Permanent fibre repair	TM	05 Nov 2026	Scheduled
A5	Update runbook RB-CONTOH-004 with the manual failover steps used on the day	Dunia Canggih NOC	07 Nov 2026	Open

We will report progress on these actions in the November Monthly Service Report.

Communications sent

TIME	TO	CHANNEL
14:11	Client IT on-call	Phone
14:20	Escalation list (IT Manager, Head of IT, Branch IT)	Email, update 1
14:50	Escalation list	Email, update 2
15:10	Escalation list	Email, closure

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

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

AI-assisted sections: alert grouping, change summary, read-only device checks, ranked causes and the first draft of the timeline. All were reviewed and edited by the NOC Lead before issue. Issued as a locked PDF within 3 working days of the incident closing. Editing is disabled; printing and copying text are allowed. This sample uses a fictional company, fictional people and mock data.

SAMPLE