Case Reference	R/E/I/147
Title	Singtel's Service Difficulty Incident on 8 October 2024 ("**Incident**")
Case Opened	8 October 2024
Case Closed	14 November 2025
Complainant	IMDA initiated this proceeding pursuant to the Code of Practice for Telecommunication Service Resiliency 2016 ("**Code**")
Respondent	Singapore Telecommunications Ltd (referred herein as "**Singtel**")
Case Summary	On 8 October 2024, a disruption to Singtel's fixed line voice service affected up to 500,000 of Singtel's residential and enterprise subscribers, between 1354 hours to 1830 hours. The Incident also affected public's access to enquiry lines and hotlines of public services, such as hospitals, medical centres, banks, government agencies, and emergency call services. The cause of the Incident was attributed to the lack of full segregation of the virtualised firewalls serving Singtel's fixed-line voice system ("**voice system**"), and Singtel's Internet-facing monitoring system for home broadband routers and Pay TV set top boxes ("**monitoring system**"). Increased intensity in Internet traffic to the monitoring system overwhelmed the shared memory resources of the firewall hardware, which was hosting the virtualised firewalls for both the voice and monitoring systems. The overwhelmed shared memory resources caused the firewalls to discard data packets intermittently, which affected the handling of calls in Singtel's voice system.
IMDA's Determination	Singtel had deployed the same firewall hardware to host separate virtualised firewalls for its voice system and monitoring system. The virtualised firewalls would protect the said systems from unauthorised access and malicious traffic. While the virtualised firewalls were separate, they shared the same memory resources of the firewall hardware. On 8 October 2024, the monitoring system encountered increased traffic intensity. The virtualised firewalls did not have

	adequate traffic filters installed to protect themselves against high intensity traffic. As a result, the increased traffic intensity to the monitoring system overwhelmed the memory resources of the firewall hardware. This affected the proper functioning of the virtualised firewalls for both the voice and monitoring systems and caused the virtualised firewall of the voice system to malfunction and operate intermittently. The intermittency of the virtualised firewall for the voice system affected the handling of voice calls. This triggered an immediate failover of voice calls to another functioning voice system at an unaffected site. However, the intermittency also caused the network traffic to flap between the two voice systems (i.e., voice traffic handling went back and forth between the two sites), leading to intermittent call dropping. The Incident was resolved after Singtel fully swung traffic over to the unaffected site. IMDA determined that the Incident could have been prevented by Singtel if it had (a) ensured full segregation of the virtualised firewalls between its voice system and its monitoring system at the firewall hardware layer, and (b) installed traffic filters in the virtualised firewalls. IMDA also determined that the incident was not due to a cyber-attack. IMDA's findings were supported by independent external consultants appointed to review the Incident. IMDA also considered that Singtel has since taken remediation measures to prevent re-occurrence of the incident. They implemented: (a) a separate firewall hardware for its voice system and its monitoring system; and (b) an intervention mechanism to stop network traffic from flapping between its sites during failovers. Nevertheless, IMDA noted that the scale and impact of the Incident was significant, as it affected the public's access to the hotlines of public services, such as hospitals, medical centres, banks, government agencies, and emergency call services. The Incident not only affected Singtel's own subscribers, but also the subscribers of other service providers who were trying to access the said hotlines and emergency call services. The potential impact on the safety and security of the public could have been very serious.

	Taking all factors into consideration, IMDA decided to impose a financial penalty of $1,000,000 on Singtel for the Incident.