Deloitte.

# LightningLink Networks Pte. Ltd.

Limited Assurance Report on X-VPN Services as of 28 February 2026

# Table of contents



**Inherent Limitations**

The procedures were performed in accordance with the engagement letter dated 21 January 2026 with LightningLink Networks Pte. Ltd. ("LightningLink Networks", or "the Company"). There are inherent limitations in any limited assurance engagement. Because of the characteristics of fraud (including computer fraud), particularly those involving concealment, misrepresentation and falsified documentation (including forgery), a properly planned and performed limited assurance engagement may not detect fraud or irregularities. In addition, a limited assurance engagement does not necessarily address the possibility that fraud may occur in the future. We have completed the assurance engagement with our procedures being designed to meet the objectives as outlined in our terms of business. Whilst due care has been exercised in the course in this project, we did not perform any investigative work which may identify additional issues other than those set out in this report. Accordingly, the issues identified and/or discussed in this report are those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made.

Due to the inherent weaknesses of any internal control system (which includes management over-ride of controls, cost benefit considerations and the possibility of collusion) and the limited scope of this limited assurance engagement, our observations should not be interpreted as a confirmation regarding the overall adequacy of the organisation's prevailing systems and/or internal controls. Our work is performed on a sample basis; we cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud.

**Limitation of Use**

This report is intended solely for the information and internal use of the Company and is not intended to be and should not be used by any other person or entity other than for submission the Company's existing clients or to the auditors duly appointed by the Company's clients. Our Report should not be referred to in any document or distributed to any other party without our prior written consent.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

**About Deloitte Singapore**

In Singapore, audit and assurance services are provided by Deloitte & Touche LLP and other services (where applicable) may be carried out by its subsidiaries and/or affiliates.

Deloitte & Touche LLP (Unique entity number: T08LL0721A) is a limited liability partnership registered in Singapore under the Limited Liability Partnerships Act 2005

Deloitte & Touche LLP
Unique Entity No. T08LL0721A
6 Shenton Way
OUE Downtown 2
#33-00
Singapore 068809

Tel: +65 6224 8288
Fax: +65 6538 6166
www.deloitte.com/sg

# Independent Practitioner's Limited Assurance Report

To the Management of LightningLink Networks Pte. Ltd.

## Scope

We have performed a limited assurance engagement on the configuration of the IT system and supporting IT operations used by LightningLink Networks Pte. Ltd. ("LightningLink Networks" or "the Company") to provide VPN services to its customers, in accordance with the Company's Statement as set out in Appendix A. Our limited assurance procedures were concluded as of 28 February 2026.

## Management Responsibilities

Management of LightningLink Networks is responsible for preparing LightningLink Networks' configuration of the IT system and supporting IT operations and the accompanying statement, including the completeness, accuracy, and method of presentation of the description, the statement, and its implementation. This is in accordance with the criteria with respect to the description of "LightningLink Networks' configuration of IT systems and management of the supporting IT operations" prepared by the Management of LightningLink Networks. This responsibility includes the design, implementation, and maintenance of the internal control system related to the preparation of LightningLink Networks' configuration of IT systems and the management of the supporting IT operations, such that they are free from material misstatement, whether due to fraud or error. Furthermore, the Management is responsible for the selection and application of the Company's Statement as set out in Appendix A.

## Our Independence and Quality Management

We have complied with the independence and other ethical requirements of *the International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants* ("IESBA") which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies *International Standard on Quality Management (ISQM) 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firms to design, implement and operate a system of quality management including policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

## Practitioner's Responsibility

Our responsibility is to perform an independent limited assurance report, and to form a conclusion on the presentation of LightningLink Networks' configuration of the IT system and management of the supporting IT operations and its implementation as set out in Appendix A.

We conducted our limited assurance engagement in accordance with International *Standard on Assurance Engagements 3000 (Revised) Assurance Engagements Other Than Audits or Reviews of Historical Financial Information* established by the International Auditing and Assurance Standards Board ("IAASB"). This standard requires that we plan and perform our procedures to form the conclusion. The extent of the procedures performed depends on our professional judgment and our assessment of the engagement risk.

Deloitte.

Our procedures include carrying out inquiries of relevant personnel of LightningLink Networks as well as examining, on a test basis, evidence supporting the configuration of the IT system and supporting IT operations and the accompanying statement. The procedures performed do not constitute a financial audit according to the International Standards on Auditing, nor an examination of compliance with laws, regulations, or other matters. Accordingly, our performance of the procedures does not result in the expression of an opinion or any other form of assurance on LightningLink Networks' compliance with laws, regulations, or other matters.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our independent limited assurance report conclusion.

Our limited assurance engagement is performed as of 28 February 2026. The procedures we performed do not provide any assurance about "LightningLink Networks' No-logs Policy" for any other period.

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement. Consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

The concept of materiality is not applied when reporting the results of control tests because Deloitte & Touche LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all exceptions.

**Inherent Limitations**

LightningLink Networks' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a company may not prevent or detect all errors or omissions in processing or reporting transactions.

**Conclusion**

Based on our procedures described in this report and evidence obtained, nothing has come to our attention that causes us to believe that LightningLink Networks' X-VPN services related IT system and IT operations as of 28 February 2026 were not prepared, in all material respects, in accordance with LightningLink Networks' statement set out in Appendix A.

**Other Matter**

Appendix B sets out the observations identified from the procedures performed. The management responses included in Appendix B have been provided by the management of LightningLink Networks in response to our observations. These management responses have not been subjected to our limited assurance procedures and accordingly, no conclusion is provided on them.

**Restriction on Distribution and Use**

Our report is solely for the purposes set forth in this report and for the information of LightningLink Networks and their customers. It is not to be used for any other purpose or to be distributed to any other parties. We do not accept or assume any liability or duty of care for any other purpose or to any other person other than LightningLink Networks' management.

Deloitte & Touche LLP

Public Accountants and
Chartered Accountants
Singapore

30 April 2026

## Appendix A: Company's Statement

LightningLink Networks Pte. Ltd. ("LightningLink Networks" or "the Company") have prepared the accompanying description on how the Company protect the privacy of the Company's customers by having effective policies and controls in place to ensure that the Company's IT systems and underlying infrastructure regarding X-VPN services are designed and implemented in line with their no-logs principles.

LightningLink Networks confirm, to the best of their knowledge and belief, that:

(a) The accompanying description fairly presents how the Company configures the IT systems and manages the supporting IT operations to ascertain that there were no logs recorded and stored that were related to customers' personal identifiable activity:

  (i) LightningLink Networks do not collect, store, or log any traffic data, including user or destination IP addresses, browsing activity, websites visited, VPN server information, DNS queries, downloaded content, or connection timestamps.

  (ii) LightningLink Networks process only the minimum account and billing information required to provide the service: a user-provided email address (not required to be verified), password stored as salted, one-way hashes (e.g., bcrypt), order ID, and order history. No additional personal information is required to create or use an account.

  (iii) LightningLink Networks collect only aggregated, non-identifiable performance metrics (e.g., CPU usage, memory consumption, and service availability) and do not collect personally identifiable information.

  (iv) User-traffic and activity logging is disabled by design: system and service outputs are redirected to a null sink (/dev/null), and controls are in place to prevent log generation or retention in production environments.

  (v) All VPN servers run entirely in RAM-only mode, meaning all data exists only in volatile memory and is never written to or cached on any physical storage. When a server is powered off, restarted, or redeployed, all data in memory is instantly and permanently erased, ensuring a true and verifiable no-logs environment.

  (vi) Production servers are deployed and managed through a predefined automation system (THA), which enforces and continuously validates the no-logs baseline configuration in production environments.

  (vii) All code changes are managed through a version-controlled CI/CD pipeline, subject to multi-level review and automated security scanning designed to validate privacy-related controls.

  (viii) Database access is protected using encrypted transmission (modern TLS) and through mutual authentication and an IP whitelist with continuous monitoring.

  (ix) The Privacy Policy is maintained to accurately reflect system operations and data processing practices, and the review, update, and publication processes are traceable and verifiable.

  (x) The Data Protection Officer ("DPO") Group operates with independence and traceability, providing ongoing oversight over privacy governance aligned with the no-logs principles.

(b) The X-VPN service is implemented as described in the description as of 28 February 2026.

In summary, LightningLink Networks' system architecture and operating controls are designed so that X-VPN service is not able to provide information about users' VPN activity as the information was not recorded or retained. LightningLink Networks do not have visibility into users' browsing history, destinations, or traffic content while using X-VPN services.

## Appendix B: Test Results, Recommendation and Management Response

**1. Manual SSH configuration changes to VPN servers should be prohibited**

| | |
|---|---|
| **Test Results** | LightningLink Network has established an Infrastructure and System Deployment Policy which requires all VPN servers to be deployed through the THA automation system and prohibits manual command-line (SSH) modifications operations.<br><br>However, it was noted that three (3) DPO personnel have been granted root-level SSH access to the production VPN servers for the purpose of oversight and performing monthly sample checks on servers' configurations.<br><br>While the access was limited to the 3 authorized DPO personnel and supported by real-time monitoring, log alert and automated rollback mechanisms for configuration changes, the root-level SSH privilege account have access to enable login and configuration capabilities outside of the THA automated deployment model. |
| **Recommendation** | Management should:<br><br>(a) Establish a formal exception process governing the use of the root-level SSH privileged account access to production X -VPN servers.<br><br>(b) Restrict the use of root-level SSH privileged account strictly to inspection or oversight activities and ensure that installation, configuration, or modification continue to be performed through the THA automated deployment framework. |
| **Management Response** | Management acknowledges the observation.<br><br>Root-level SSH access was granted to three (3) DPO personnel for the specific purpose of enabling independent oversight of no-logs controls and timely performance of oversight responsibilities.<br><br>To ensure the secure and compliant use of such access, management implemented strict monitoring and mitigating controls, including audit logging, real-time monitoring and alerting, and an automated rollback mechanism for configuration changes. Management has not identified any unauthorized, unapproved, or otherwise non-compliant activities. However, notwithstanding these controls, root-level SSH privileges still present residual risk, as noted in the observation.<br><br>Upon identification of the observation, management immediately revoked root-level SSH access for DPO personnel, thereby fully prohibiting manual SSH access to the production servers. DPO oversight and review activities previously are now performed through the THA automated audit process. These corrective actions were completed on February 4, 2026, and owned by the Engineering Manager. |
| **Implementation Date** | 04 February 2026 (Completed) |

**2. Database schema changes should be approved by designated DPO personnel with segregation of duties**

| | |
|---|---|
| **Test Results** | LightningLink Network had established a Data Protection, Minimization and Retention Policy which requires all system configuration changes and database schema changes to obtain dual approval from at least two designated DPOs.<br><br>However, it was noted that one (1) database change request dated 11 December 2025 was approved by two non-DPO personnel.<br><br>In addition, one of the approvers was the same individual who submitted the change request. |
| **Recommendation** | Management should:<br><br>(a) Check that all database schema and system configuration changes obtain dual approval from designated DPO personnel.<br><br>(b) Check that there is segregation of duties within the approval workflow and that requestor are prohibited from self-approve their own change requests. |
| **Management Response** | Management acknowledges the observation.<br><br>Management's retrospective review determined that the record dated 11 December 2025 was a test record generated during internal testing of the DPO oversight system by the engineering team to verify that the system was operating properly. The record was not removed after testing. It did not represent an actual production approval process, and the specific change was not implemented. The review identified this as an isolated record and confirmed that other production changes followed the required submission and approval process.<br><br>However, the review also confirmed that the system was not operating as intended. Upon identification of the observation, management performed a comprehensive remediation of the DPO oversight system.<br><br>The system has since been updated to implement the policy-defined dual-DPO approval requirement and to maintain appropriate segregation of duties between requestor and approver. These corrective actions were completed on February 4, 2026, and owned by the Reliability Engineering Team Lead. |
| **Implementation Date** | 04 February 2026 (Completed) |