

STARHUB'S SERVICE SPECIFIC TERMS & CONDITIONS SME FIREWALL

Effective as of [June 2026]

The StarHub SME Firewall Service refers to firewall and/or managed firewall services for small and medium enterprises requiring firewall hardware, firewall subscription, firewall management, security policy configuration, monitoring, support, and related services on a subscription plan.

These StarHub SME Firewall Specific Terms and Conditions ("SME Firewall Service Terms") set out the basis on which StarHub Ltd. ("StarHub", "we", "us", "our") will provide the SME Firewall Service to you.

These SME Firewall Service Terms shall be read in conjunction with StarHub's Business General Terms and Conditions ("Business General Terms & Conditions"), the applicable Service Application Form ("SAF"), quotation, order form, Scope of Work ("SOW"), and any other applicable documents agreed between StarHub and the Customer in writing.

In the event of any conflict or inconsistency, the order of precedence shall be as set out in the Business General Terms & Conditions, unless otherwise agreed by StarHub in writing.

1. Definitions and Interpretation

1.1. In these SME Firewall Service Terms, unless the context otherwise requires:

"Agreement" means the signed SAF, quotation, SOW, these SME Firewall Service Terms, the Business General Terms & Conditions, and any other terms agreed between StarHub and the Customer in writing.

"Business Hours" means Monday to Friday, excluding Singapore public holidays, from 9.00am to 6.00pm Singapore time.

"Charges" means all monthly recurring charges, one-time charges, installation charges, delivery charges, professional service charges, managed service charges, licence charges, subscription charges, administrative charges, early termination charges, and any other fees payable by the Customer for or relating to the Service.

"Customer" means the company, business, or organisation that applies for and/or subscribes to the Service from StarHub. "You" and "your" shall have the corresponding meaning.

"Firewall Equipment" means any firewall appliance, router, security gateway, virtual firewall, power adapter, accessory, software, licence, subscription, agent, or related equipment supplied, leased, supported, or managed as part of the Service.

"Firewall Service" or "Service" means the StarHub SME Firewall Service, including firewall hardware, firewall subscription, managed firewall, firewall monitoring, configuration, support, reporting, and/or other services set out in the SAF, quotation, order form, and/or SOW.

"Managed Firewall" means the firewall management service provided by StarHub and/or its authorised service delivery partner, which may include configuration, monitoring, policy changes, firmware support, remote troubleshooting, and reporting.

“MyRepublic” means MyRepublic Broadband Pte. Ltd., appointed by StarHub as its authorised service delivery partner for the Service, where applicable.

“Professional Service” means onsite or remote setup, installation, configuration, deployment, migration, firewall policy setup, troubleshooting, or other professional services required by the Customer and agreed in the SOW.

“Security Policy” means firewall rules, access rules, routing rules, NAT rules, VPN settings, filtering policies, security profiles, and any other configuration applied to the Firewall Equipment.

“SOW” means the Scope of Work applicable to the Service.

“Third-Party Provider” means any manufacturer, distributor, vendor, software provider, security provider, maintenance provider, logistics provider, or other third party involved in the provision of the Service.

1.2. For interpretation:

- 1.2.1. words importing the singular include the plural and vice versa;
- 1.2.2. headings are inserted for convenience only and do not affect interpretation;
- 1.2.3. “include”, “includes”, and “including” mean “including without limitation”; and
- 1.2.4. any reference to any statute or regulation includes such statute or regulation as amended, replaced, or re-enacted.

2. **Scope of Service**

- 2.1. StarHub agrees to provide, and the Customer agrees to take and pay for, the Service as set out in the applicable SAF, quotation, order form, and/or SOW.
- 2.2. The Service may include one or more of the following:
 - 2.2.1. supply of Firewall Equipment;
 - 2.2.2. firewall installation and basic configuration;
 - 2.2.3. firewall policy setup;
 - 2.2.4. remote firewall management;
 - 2.2.5. firewall rule changes;
 - 2.2.6. firmware update support;
 - 2.2.7. VPN configuration support;
 - 2.2.8. firewall health monitoring;

- 2.2.9. firewall alert monitoring;
- 2.2.10. Reporting;
- 2.2.11. onsite support, where expressly included in the SOW; and
- 2.2.12. Any other service expressly agreed by StarHub in writing.
- 2.3. Unless expressly stated in the SOW, the Service does not include:
 - 2.3.1. cybersecurity incident response;
 - 2.3.2. forensic investigation;
 - 2.3.3. malware removal from endpoints or servers;
 - 2.3.4. penetration testing;
 - 2.3.5. vulnerability assessment;
 - 2.3.6. compliance audit or certification;
 - 2.3.7. security awareness training;
 - 2.3.8. endpoint protection;
 - 2.3.9. email security;
 - 2.3.10. data backup or recovery;
 - 2.3.11. application troubleshooting unrelated to firewall configuration;
 - 2.3.12. LAN cabling, electrical works, rack works, or site preparation;
 - 2.3.13. support for non-StarHub subscribed firewall equipment;
 - 2.3.14. SIEM, SOC, MDR, or 24x7 security monitoring, unless expressly included;
 - 2.3.15. remediation of Customer vulnerabilities; or
 - 2.3.16. any service not expressly stated in the SOW.
- 2.4. The Customer accepts that it is responsible for ensuring that the Service is suitable for its business needs.
- 3. **Application and Eligibility**
 - 3.1. The Customer may apply for the Service through StarHub's authorised representative, in person or in writing, using StarHub's latest application forms or order process.
 - 3.2. To be eligible for the Service, the Customer must:
 - 3.2.1. be an entity registered with the Accounting and Corporate Regulatory Authority of

Singapore or have a valid Singapore Unique Entity Number;

- 3.2.2. satisfy StarHub's credit policy;
 - 3.2.3. not have outstanding debt with StarHub, unless otherwise accepted by StarHub;
 - 3.2.4. provide details of an authorised contact person with a valid email address and contact number;
 - 3.2.5. provide accurate and complete information required for credit, risk, technical, and service Assessment;
 - 3.2.6. provide accurate network, site, IP addressing, application, and security requirement Information;
 - 3.2.7. not have previously misused StarHub's services; and
 - 3.2.8. where required by StarHub, provide a Directors' Guarantee, security deposit, or other form of Security.
- 3.3. StarHub may request additional documentation, completed questionnaires, network diagrams, site information, firewall rule requirements, VPN requirements, or other information as part of the application assessment.
 - 3.4. StarHub may verify the Customer's identity, credit status, and risk profile with authorised bodies, suppliers, and credit reference agencies. The Customer authorises StarHub to carry out such checks.
 - 3.5. StarHub may accept or reject any application at its sole discretion and shall not be liable to the Customer for any rejection.
 - 3.6. StarHub may impose additional conditions when accepting an application, including credit limits, security deposits, payment terms, minimum contract period, or other requirements.

4. Service Lead Time and Activation

- 4.1. The service lead time shall be as stated in the SOW or as advised by StarHub's representative.
- 4.2. The lead time is subject to Firewall Equipment availability, licence availability, resource availability, technical readiness, site readiness, access, Customer cooperation, and procurement of all relevant approvals.
- 4.3. StarHub shall not be liable for any delay caused by events outside its reasonable control, including third-party delay, manufacturer delay, stock shortage, logistics delay, Customer delay, incomplete information, site readiness issues, or delayed approval from the Customer.
- 4.4. If StarHub is unable to meet the requested service activation date, StarHub may provide an alternative date in writing.
- 4.5. If the Customer cancels an accepted application, order, or project after StarHub has commenced processing, cancellation charges may apply.

5. Firewall Equipment Ownership, Leasing, and Usage

- 5.1. Where the Service includes Firewall Equipment supplied under a leasing or subscription arrangement, ownership of the Firewall Equipment shall remain with StarHub, its authorised service delivery partner, or the applicable Third-Party Provider, unless otherwise stated in the SAF, quotation, or SOW.
- 5.2. The Customer shall take due care of the Firewall Equipment and shall keep the Firewall Equipment in good condition, fair wear and tear excepted.
- 5.3. The Customer shall not dismantle, remove parts from, tamper with, modify, reset, relocate, sell, assign, pledge, transfer, or dispose of the Firewall Equipment without StarHub's prior written approval.
- 5.4. The Customer shall bear the cost of any loss, theft, damage, misuse, unauthorised modification, or failure to return the Firewall Equipment.
- 5.5. If the Firewall Equipment is lost or damaged and such loss or damage is not covered by the applicable manufacturer warranty, the Customer shall pay the replacement cost of the Firewall Equipment and any related delivery, installation, administrative, or recovery charges.
- 5.6. StarHub may supply refurbished Firewall Equipment, provided such Firewall Equipment is tested to be in good working order and reset to factory default settings before delivery.
- 5.7. StarHub may replace the Firewall Equipment with another firewall of similar or equivalent specification where required for service fulfilment, stock availability, warranty replacement, or operational reasons.
- 5.8. StarHub may remotely install, update, upgrade, patch, configure, or remove software, firmware, subscriptions, licences, settings, or tools on the Firewall Equipment from time to time for the purpose of providing the Service.

6. Delivery, Installation, and Deployment

- 6.1. StarHub will deliver the Firewall Equipment to the installation or delivery address provided by the Customer.
- 6.2. The Customer shall ensure that the installation or delivery address is accurate, valid, accessible, and authorised.
- 6.3. The Customer shall ensure that the site is ready for installation, including rack space, power supply, internet connectivity, cabling, cooling, physical access, and any required approvals.
- 6.4. Delivery, installation, and deployment shall be carried out during Business Hours, unless otherwise agreed by StarHub in writing.
- 6.5. Delivery, installation, deployment, or support outside Business Hours, on weekends, on the eve of public holidays, or on public holidays may be subject to additional charges.

- 6.6. Unless expressly stated in the SOW, delivery and deployment do not include:
 - 6.6.1. project management;
 - 6.6.2. migration planning;
 - 6.6.3. complex network redesign;
 - 6.6.4. data migration;
 - 6.6.5. user training;
 - 6.6.6. advanced security policy design;
 - 6.6.7. application troubleshooting;
 - 6.6.8. LAN cabling or electrical works; or
 - 6.6.9. configuration of features not listed in the SOW.
- 6.7. Any additional site visit, engineer visit, or support request caused by Customer delay, incomplete information, site readiness issues, user unavailability, inaccurate network information, or out-of-scope requirements may be chargeable.

7. Firewall Configuration and Security Policy

- 7.1. StarHub will configure the Firewall Equipment based on information, requirements, rules, and approvals provided by the Customer.
- 7.2. The Customer is responsible for ensuring that all firewall rules, ports, IP addresses, applications, VPN users, NAT rules, routing requirements, and access requirements provided to StarHub are accurate, complete, authorised, and suitable for the Customer's business.
- 7.3. The Customer shall nominate authorised personnel to approve firewall changes and Security Policies.
- 7.4. StarHub may reject, delay, or request clarification for any firewall rule, access request, whitelisting request, or Security Policy that is incomplete, unclear, insecure, technically unsuitable, unlawful, or likely to cause service disruption or security risk.
- 7.5. The Customer remains responsible for the business impact and security impact of firewall rules, access exceptions, whitelisting, VPN access, and configurations requested or approved by the Customer.
- 7.6. StarHub shall not be liable for any outage, access issue, blocked traffic, degraded performance, security exposure, application issue, or business interruption arising from inaccurate information, incomplete requirements, Customer-approved rules, legacy configuration, third-party network changes, or Customer delay.

8. Managed Firewall Monitoring and Management

- 8.1. StarHub and/or its authorised service delivery partner may provide monitoring and management for Firewall Equipment subscribed under the Service.
- 8.2. StarHub will only monitor and manage Firewall Equipment expressly covered under the Service.
- 8.3. Where monitoring is included, StarHub may monitor firewall availability, health status, alerts, or other parameters stated in the SOW.
- 8.4. Monitoring does not mean that StarHub will detect, investigate, stop, prevent, or remediate all threats, attacks, vulnerabilities, misconfigurations, outages, or abnormal activities.
- 8.5. The Customer may request configuration or firewall rule changes during the contract period, subject to StarHub's approval.
- 8.6. Change requests must be submitted by the Customer's authorised contact through the support channel designated by StarHub.
- 8.7. StarHub will assess each change request and may confirm the impact on implementation timeline, Charges, service scope, and applicable terms.
- 8.8. Unless otherwise stated in the SOW, change requests shall be implemented remotely at a mutually agreed time.

9. Firmware, Licences, and Subscriptions

- 9.1. Where included in the Service, StarHub may assist with firmware updates, security updates, patches, licence renewals, and subscription management for the Firewall Equipment.
- 9.2. Firmware updates, patches, and licence renewals are subject to availability from the applicable manufacturer or Third-Party Provider, compatibility, vendor support status, maintenance window, Customer approval, and network readiness.
- 9.3. The Customer acknowledges that firmware updates, patches, licence changes, or configuration changes may cause downtime, compatibility issues, traffic disruption, VPN issues, routing issues, or performance impact.
- 9.4. StarHub shall not be responsible for issues caused by unsupported equipment, end-of-life equipment, expired licences, Customer delay, Customer refusal to approve updates, third-party software conflicts, internet service issues, power issues, or any matter outside StarHub's reasonable control.
- 9.5. Unless otherwise stated in the SAF, quotation, or SOW, licences, subscriptions, renewals, security bundles, threat intelligence feeds, advanced security features, and vendor support are chargeable separately.

10. Customer and Technical Support

STARHUB'S SERVICE SPECIFIC TERMS & CONDITIONS
SME FIREWALL

- 10.1. StarHub provides remote technical support during Business Hours, unless otherwise stated in the SOW.
- 10.2. For security and accountability purposes, StarHub will only provide assistance to the authorised officers listed in the Customer's application or subsequently notified to StarHub in writing.
- 10.3. The Customer shall provide physical and/or remote access to the Firewall Equipment for support purposes.
- 10.4. StarHub may require the Customer to assist with troubleshooting before onsite support is arranged.
- 10.5. If StarHub is unable to resolve a fault remotely, StarHub may arrange onsite support during Business Hours, subject to resource availability and the scope of the Service.
- 10.6. Onsite response times may vary depending on location, spare parts availability, engineer availability, manufacturer support, and other operational factors.
- 10.7. The Customer shall provide the authorised technician with safe access to the Customer's premises, Firewall Equipment, electricity, internet connection, rack, cabling, and sufficient working space.
- 10.8. If the Firewall Equipment fails during normal and proper use within the applicable coverage period, StarHub may repair or replace the defective parts or Firewall Equipment with new or reconditioned parts or products that are functionally equivalent or superior.
- 10.9. If the Firewall Equipment is found to be outside the support or warranty coverage scope, StarHub may provide a chargeable quotation before proceeding. If the Customer does not proceed, StarHub may charge the Customer for costs already incurred, including engineer dispatch, testing, troubleshooting, and administrative costs.

11. Security Limitation

- 11.1. The Customer acknowledges that firewall services are one component of cybersecurity and cannot guarantee complete protection.
- 11.2. StarHub does not warrant that the Service will:
 - 11.2.1. prevent all cyberattacks, malware, ransomware, phishing, unauthorised access, data loss, or security breaches;
 - 11.2.2. detect all vulnerabilities, threats, malicious activities, misconfigurations, or abnormal traffic;
 - 11.2.3. ensure compliance with any law, regulation, framework, audit requirement, or industry Standard;
 - 11.2.4. prevent downtime, degraded performance, or network interruption; or
 - 11.2.5. Make the Customer's systems fully secure.
- 11.3. The Customer remains responsible for its overall cybersecurity posture, including endpoint

security, email security, user awareness, password management, identity and access management, backup, application security, cloud security, data protection, incident response, policies, and compliance obligations.

12. Logs, Data, and Privacy

- 12.1. The Customer acknowledges that the Service may involve processing of firewall logs, IP addresses, user identifiers, URLs, domain names, security events, traffic metadata, device information, configuration data, ticket information, and other technical data.
- 12.2. The Customer shall ensure that it has obtained all necessary consents and provided all necessary notices to its employees, contractors, users, and representatives for StarHub and its authorised service delivery partners to access, process, use, store, or disclose such data as required to provide the Service.
- 12.3. StarHub may use such data to provide, manage, support, bill, secure, troubleshoot, report on, improve, or maintain the Service.
- 12.4. Unless expressly agreed in writing, StarHub is not responsible for long-term log retention, forensic preservation, compliance reporting, or legal hold.

13. Third-Party Providers and Vendor Terms

- 13.1. The Service may involve Firewall Equipment, software, licences, subscriptions, maintenance, support, or cloud services provided by Third-Party Providers.
- 13.2. The Customer shall comply with all applicable Third-Party Provider terms, end-user licence agreements, acceptable use policies, export restrictions, and service terms.
- 13.3. StarHub shall not be responsible for any suspension, termination, vulnerability, defect, limitation, price change, licence change, feature change, end-of-life announcement, or discontinuation of any third-party product or service.
- 13.4. Where a Third-Party Provider changes its pricing, licensing model, features, support terms, or service terms, StarHub may adjust the Charges, scope, or terms of the Service by giving notice to the Customer.

14. Acceptable Use Restrictions

- 14.1. The Customer must not use the Service or Firewall Equipment:
 - 14.1.1. in any unlawful manner or for any unlawful purpose;
 - 14.1.2. fraudulently or maliciously;
 - 14.1.3. to hack into, disrupt, damage, or compromise any system;
 - 14.1.4. to insert malicious code, viruses, malware, or harmful data;

14.1.5. In a way that could damage, disable, overburden, impair, or compromise StarHub's systems, security, network, or services;

14.1.6. in a way that interferes with other users or customers; or

14.1.7. to bypass, evade, or undermine security controls.

14.2. StarHub may determine, at its sole discretion, whether the Customer has breached this Clause.

15. Charges and Payment

15.1. The Customer shall pay all Charges for the Service in accordance with the Agreement.

15.2. Charges may include monthly recurring charges, one-time charges, installation charges, delivery charges, firewall equipment charges, licence charges, subscription charges, managed service charges, professional service charges, administrative charges, out-of-scope support charges, replacement charges, and early termination charges.

15.3. Charges shall commence from the service activation date, delivery date, deployment date, installation date, or such other date stated in the SAF, quotation, or SOW.

15.4. Unless otherwise agreed in writing, all Charges are non-refundable.

15.5. Any request for additional sites, additional Firewall Equipment, upgraded firewall models, higher throughput, additional licences, additional security subscriptions, additional VPN users, onsite service, after-hours support, configuration changes, incident support, or out-of-scope work may be subject to additional Charges.

16. Suspension and Recovery of Firewall Equipment

16.1. StarHub may suspend the Service if the Customer fails to pay any Charges when due.

16.2. If payment remains outstanding for two consecutive months, StarHub or its authorised service delivery partner may require the Customer to return the Firewall Equipment.

16.3. The Customer shall return the Firewall Equipment within fourteen days from StarHub's request.

16.4. If the Firewall Equipment is not returned within the required period, StarHub or its authorised service delivery partner may take further action to recover the Firewall Equipment and/or report the missing Firewall Equipment to the relevant authorities.

16.5. The Customer shall remain liable for all outstanding Charges, Firewall Equipment replacement costs, recovery costs, administrative costs, and any other amounts payable under the Agreement.

17. Termination of Service

STARHUB'S SERVICE SPECIFIC TERMS & CONDITIONS
SME FIREWALL

- 17.1. The Service shall continue for the contract period stated in the SAF, quotation, order form, or SOW.
- 17.2. The Customer shall not terminate the Service before the end of the agreed contract period, unless StarHub agrees in writing.
- 17.3. StarHub may terminate all or any part of the Service with immediate effect without compensation if:
 - 17.3.1. the Customer breaches any term of the Agreement;
 - 17.3.2. the Customer fails to make payment for two consecutive months;
 - 17.3.3. the Customer becomes or threatens to become bankrupt, insolvent, wound up, dissolved, placed under judicial management, receivership, administration, or liquidation;
 - 17.3.4. the Customer makes any arrangement with creditors;
 - 17.3.5. the Customer provides incorrect, false, or incomplete information;
 - 17.3.6. the Customer misuses the Service;
 - 17.3.7. the Customer is likely to create imminent harm to StarHub's network, systems, services, personnel, or other customers; or
 - 17.3.8. the Customer acts fraudulently, maliciously, abusively, or unlawfully.
- 17.4. Upon expiry or termination of the Service, the Customer must return all Firewall Equipment to StarHub or its authorised service delivery partner within two weeks, unless StarHub confirms in writing that the Customer may retain the Firewall Equipment.
- 17.5. Alternatively, subject to StarHub's approval, the Customer may purchase and retain the Firewall Equipment by paying the full firewall equipment cost and any applicable Charges.
- 17.6. StarHub may invoice an additional termination or recovery charge of S\$200 per Firewall Equipment if:
 - 17.6.1. the Firewall Equipment is not returned;
 - 17.6.2. the Firewall Equipment is returned incomplete;
 - 17.6.3. the Firewall Equipment is defective upon return;
 - 17.6.4. accessories, power adaptors, cables, or parts are missing; or
 - 17.6.5. the Firewall Equipment is not returned within the required period.
- 17.7. The Customer shall remain responsible for maintaining its own firewall, network security, internet connectivity, business continuity, and security operations after termination or expiry of the Service.

18. Early Termination

- 18.1. If the Customer terminates, cancels, downgrades, reduces, or fails to continue the Service before the end of the agreed contract period, early termination charges shall apply.
- 18.2. The early termination charge shall be the total sum of the monthly recurring charges for the remaining months of the applicable contract period.
- 18.3. In addition to the early termination charge, the Customer shall pay:
 - 18.3.1. all outstanding Charges up to the effective date of termination;
 - 18.3.2. all unpaid Firewall Equipment charges;
 - 18.3.3. all unpaid managed service charges;
 - 18.3.4. all unpaid licence and subscription charges;
 - 18.3.5. all unpaid installation, delivery, administrative, or professional service charges;
 - 18.3.6. any applicable third-party charges;
 - 18.3.7. replacement costs for lost, damaged, or unreturned Firewall Equipment; and
 - 18.3.8. any other amounts payable under the Agreement.
- 18.4. For avoidance of doubt, the Customer remains liable to pay the full remaining contract value for the unexpired portion of the contract period, whether or not the Customer continues to use the Service.

19. Audit

- 19.1. StarHub may inspect or appoint an accountant, auditor, or authorised representative to inspect the Firewall Equipment and records relating to the Service and the Customer's compliance with the Agreement.
- 19.2. Any audit shall be conducted during the Customer's normal business hours and in a manner that does not materially interfere with the Customer's normal business operations.
- 19.3. The Customer shall provide reasonable assistance for such an audit.
- 19.4. If an audit reveals that the Customer is in breach of the Agreement, the Customer shall:
 - 19.4.1. reimburse StarHub for the actual costs and expenses of the audit; and
 - 19.4.2. compensate StarHub for any unauthorised use, loss, damage, or misuse of the Firewall Equipment.

20. Revision

STARHUB'S SERVICE SPECIFIC TERMS & CONDITIONS
SME FIREWALL

- 20.1. StarHub reserves the right to change, amend, or revise these SME Firewall Service Terms.
- 20.2. The revised SME Firewall Service Terms shall become effective once posted on StarHub's website or otherwise notified to the Customer.
- 20.3. The Customer's continued use of the Service shall constitute acceptance of the revised SME Firewall Service Terms.