

**SINGAPORE INTERNET
EXCHANGE (SGIX)**

Draft Policies and Procedures

1. PURPOSE OF THIS DOCUMENT	4
2. DEFINITIONS	4
3. OPERATIONS POLICY	5
3.1 Purpose	5
3.2 Terms of policy	5
3.2.1 General management.....	5
3.2.2 Policies and Procedures.....	5
3.2.3 Joining and peering	5
3.2.4 Communication	5
3.2.5 Responsibility to monitor Members	6
4. NON-COMPLIANCE POLICY	7
4.1 Purpose	7
4.2 Terms of policy	7
4.2.1 Violation of Policies and Procedures	7
5. MEMBERSHIP POLICY	8
5.1 Purpose	8
5.2 Terms of policy	8
5.2.1 General	8
5.2.2 Conditions that must be met by new applicants	8
5.2.3 Conditions that must be maintained by all Members	8
5.2.4 Members responsibilities.....	8
6. FEES AND PAYMENT POLICY	10
6.1 Purpose	10
6.2 Terms of policy	10
6.2.1 General	10
6.2.2 Payment and invoicing terms	10
6.2.3 Penalties for non-payment.....	11
6.2.4 Pricing mechanism	11
7. TECHNICAL REQUIREMENTS POLICY	13
7.1 Purpose	13
7.2 Terms of policy	13
7.2.1 General	13
7.2.2 Physical interfaces	13
7.2.3 MAC layer.....	13
7.2.4 IP layer	14
7.2.5 Routing	14
7.2.6 Forwarding	15

8. ACCEPTABLE USE POLICY	16
8.1 Purpose	16
8.2 Terms of policy	16
8.2.1 General	16
8.2.2 Prevention of network flooding and denial-of-service attacks	16
8.2.3 Unauthorised access or malicious attempts to compromise the SGIX network	16
8.2.4 Illegal traffic	17
9. JOINING AND CONNECTION PROCEDURE	18
9.1 Purpose	18
9.2 Terms of procedure	18
9.2.1 Application for membership	18
9.2.2 Connection	19
9.2.3 Report setup	19
10. DISCONNECTION PROCEDURE (NON-COMPLIANCE)	20
10.1 Purpose	20
10.2 Terms of procedure	20
10.2.1 Reasons for disconnection	20
10.2.2 Enquiry into forced disconnection based on non-compliance with Policies and Procedures	21
10.2.3 Disconnection	21
11. DISCONNECTION PROCEDURE (VOLUNTARY)	22
11.1 Purpose	22
11.2 Terms of procedure	22
11.2.1 Notification of Member's intention to disconnect	22
11.2.2 Disconnection	22

1. Purpose of this document

This document sets out the policies and procedures of SGIX.

2. Definitions

The following definitions are used throughout this document.

“SGIX”	the Singapore Internet Exchange
“Company”	the company operating SGIX, a company limited by guarantee and incorporated in Singapore
“Board”	the board of directors of the Company
“Management”	the management and staff of SGIX, and any third party empowered by the management or staff of SGIX to act in their stead.
“MAA”	the Memorandum and Articles of Association of the Company
“Policies and Procedures”	the policies and procedures governing the operation of SGIX, as detailed in this document
”Member”	a member of the Company
“Peering Fabric”	the network infrastructure of SGIX

3. Operations policy

3.1 Purpose

1. To ensure that the Management and the Board govern SGIX in accordance with best-practices acceptable within the global community of IXP operators.

3.2 Terms of policy

3.2.1 General management

1. The Management shall conduct the day-to-day affairs of SGIX. The Management shall be overseen by the Board.

3.2.2 Policies and Procedures

1. The Policies and Procedures shall be made publicly available on the SGIX website.
2. The Board and the Management may, from time to time, recommend changes to the Policies and Procedures.
3. Policies and Procedures may be changed or implemented at the discretion of the Board, except in cases where the MAA states that the Policy or Procedure in question is a reserved matter.

3.2.3 Joining and peering

1. SGIX shall not:
 - a. deny membership to any organisation that meets the prerequisites specified in the Membership Policy;
 - b. make any policy or restrictions on the bilateral or multilateral relationships or transactions which the Members may form between each other. SGIX shall not be held liable for any breach of contract or service level agreement between a Member and a third party or between Members.

3.2.4 Communication

1. The primary means of communication between SGIX and its Members will be via email.
2. SGIX shall ensure that Members are provided with a valid, 24/7 operational contact.

3.2.5 Responsibility to monitor Members

1. SGIX shall ensure that Members comply with the conditions for membership as set out in the Membership Policy.
2. SGIX shall ensure that the Members:
 - a. abide by the Policies and Procedures;
 - b. refer any problems, issues and concerns in a timely and appropriate manner so as to enable quick resolution and reduce risk to the operations of SGIX;
 - c. conduct their activities in SGIX in a manner that is not detrimental to the other Members;
 - d. do not carry out any illegal activities through SGIX.
3. SGIX shall monitor any port where:
 - a. the information is required by law;
 - b. the information gathered is generic in nature and is solely used for statistical or network management purposes;
 - c. the information is necessary to determine that the Members are exchanging traffic as required by the Membership Policy.
4. SGIX shall make reasonable efforts to ensure that any monitoring will neither adversely affect the services rendered to a Member nor compromise Member confidentiality.

4. Non-compliance policy

4.1 Purpose

1. To define the rights and responsibilities of the SGIX in the event of non-compliance by a Member

4.2 Terms of policy

4.2.1 Violation of Policies and Procedures

1. All Members shall comply with the Policies and Procedures.
2. SGIX reserves the right to investigate suspected violations of the Policies and Procedures. SGIX may also initiate an investigation, which may include gathering information from the parties involved.
3. If SGIX, at its sole discretion, decides that a violation has occurred, it may choose to take necessary corrective action.
4. It may determine what action to take on a case-by-case basis. Such action may include, but is not limited to, temporary disconnection from the Peering Fabric or termination of membership. For details, refer to the Disconnection Procedure (Non-Compliance).
5. SGIX will inform the Member of the intentions to investigate, the actions to be taken against the non-compliance, and the anticipated period of distribution, if any.
6. Violations of the Policies and Procedures may also subject the Member to criminal or civil liability.
7. If a Member is temporarily disconnected for a period of 24 hours or longer, pending investigation into an alleged breach, the Member is not liable to pay fees and charges for the period of temporary disconnection. Payment shall resume if temporary disconnection ends with the reinstatement of membership rights and reconnection.

5. Membership policy

5.1 Purpose

1. To detail the prerequisites for membership of the Company and ongoing responsibilities of the Members

5.2 Terms of policy

5.2.1 General

1. In order to purchase services from SGIX, an organisation must be a Member of the Company

5.2.2 Conditions that must be met by new applicants

1. It is intended that only organisations with a legitimate interest in exchanging Internet traffic be admitted to membership of the Company. The conditions set out below must be met prior to admission of new Members.
 - a. New applicants must have an Autonomous System Number (ASN) as assigned by a Regional Internet Registry.
 - b. New applicants must have the intention to, and be willing to agree to the MAA.
 - c. Upon the applicant's agreement to the MAA, Members must exchange traffic with at least one other Member within three months.

5.2.3 Conditions that must be maintained by all Members

1. The conditions set out below must be maintained at all times by existing Members.
 - a. Members must subscribe to at least one port connection from SGIX.
 - b. Members must have an Autonomous System Number (ASN) as assigned by a Regional Internet Registry.
 - c. Members must at all times adhere to the Policies and Procedures.
 - d. Members must exchange traffic with at least one other Member.

5.2.4 Members responsibilities

1. Members shall provide 24/7 operational contact details for use by the Management and other Members. Assigned contacts shall have the ability to understand spoken

and written English and shall understand the requirements of the Policies and Procedures and MAA.

2. Members must ensure all contact information held by SGIX is up to date and accurate.
3. Members shall provide an email address to which requests for peering, and other communications, should be sent.
4. Members shall not refer their customers or any agent of their customers, directly to SGIX unless sanctioned by the Management.
5. Members must subscribe to email mailing lists and other communications channels as determined by the Management.
6. Members must not disclose confidential information of other Members to a third party.

6. Fees and payment policy

6.1 Purpose

1. To set out payment terms for services rendered by SGIX, penalties for non-payment, and policies regarding pricing changes.
2. To ensure that pricing is on a cost recovery basis and ensures sufficient reserves to be built up to enable effective functioning of SGIX.

6.2 Terms of policy

6.2.1 General

1. All Members have the responsibility to settle payments for services rendered by SGIX according to the guidelines set out in this policy.

6.2.2 Payment and invoicing terms

1. SGIX will charge Members on a monthly basis for port connectivity.
2. SGIX will charge Members on a one-off basis for the following services:
 - a. Installation and configuration of ports;
 - b. Installation and configuration of link aggregation. In order to subscribe to the link aggregation service, a Member must purchase two or more ports to be used in conjunction with this service;
 - c. Installation and configuration of private peering using the IEEE 802.1q standard. In order to subscribe to the private peering service using the IEEE 802.1q standard, a Member must purchase one or more ports to be used in conjunction with this service.
3. All monthly charges will be invoiced in advance on the first working day of the month of service.
4. All one-off installation charges will be invoiced on the day of service provision.
5. All invoices must be paid within thirty days of issue.
6. All services are purchased for a minimum period of one month.
7. Monthly fees shall be pro-rated in the following circumstances:
 - a. A Member joins part way through a month;
 - b. A Member's port is disconnected for a period of greater than 24 hours due to non-compliance.

6.2.3 Penalties for non-payment

1. Following the due date as stated in the invoice, Members will be charged interest pursuant to 3-month Singapore Interbank Offered Rate (SIBOR) plus 8 percentage points on any balance outstanding.
2. If the invoice has not been settled in full following 90 days from the date of issue, the Member will be considered to be in default, and in violation of this policy. This may result in actions being taken as per stated in the Non-Compliance Policy.

6.2.4 Pricing mechanism

1. The pricing of services in SGIX is on a cost recovery basis.
2. The general procedure for calculating prices is as follows:
 - a. Prices are reviewed once per year, when the financial accounts are available;
 - b. Direct costs of offering a service are allocated to each service;
 - c. Overhead costs are allocated to each service in proportion to the total direct costs of each service;
 - d. For each service, allocated overhead costs and direct costs are added to calculate the total cost of offering that service;
 - e. The total cost of the service is allocated according to the quantity supplied of the service to obtain the unit cost of the service;
 - f. A margin is applied to the unit cost of the service, based on the retained surpluses recorded in the financial statements of the immediate previous financial year. If the previous year's retained surplus is below SGD 500,000, then the margin is equal to 5%. Otherwise the margin is equal to the retained surplus threshold (SGD 500,000), minus the retained surplus at the end of the previous financial year, divided by total operating expense as stated in the previous year's financial statements. The minimum margin shall be -20% in the case when the retained surplus is above the threshold value;
 - g. Should the opinion of the Board be that the calculated cost recovery price is too high, a percentage discount may be applied to the resultant prices, to be applied equally across all services, at the discretion of the Board.
3. Costs are allocated to monthly port charges as follows:
 - a. Direct costs of offering port capacity are allocated to ports. This includes the monthly rental and up-front installation cost of leased lines between nodes, depreciation of Ethernet switches, depreciation of servers and related equipment, costs of the SGIX website, and licence fees of SGIX;

- b. Total direct and overhead costs are allocated to ports such that the ratio of unit costs for 10Gbit/s port to 1Gbit/s port to 100 Mbit/s port shall be equal to 10.0:2.7:1.0.
4. Direct costs are allocated to charges for installation and configuration of ports as follows:
 - a. Direct labour required to install and configure ports shall be allocated to new port configurations.
5. Direct costs are allocated to charges for installation and configuration of link aggregation as follows:
 - b. Direct labour required to configure link aggregation activation requests shall be allocated to new link aggregation configurations.
6. Direct costs are allocated to charges for installation and configuration of private peering using the IEEE 802.1q standard as follows:
 - a. Direct labour required to configure private peering using the IEEE 802.1q standard activation requests shall be allocated to new private peering configurations using the IEEE 802.1q standard.
7. Overhead costs shall be allocated to all services in proportion to direct costs of each service. These include the following:
 - a. Sales and marketing costs;
 - b. Staff costs less the cost of direct labour for the configuration of ports, link aggregation and private peering using the IEEE 802.1q standard;
 - c. Corporate secretarial and administrative costs;
 - d. Office expenses including rental of property, stocking of office and maintenance of fixtures and fittings;
 - e. Cost of maintenance and statistics services, and network operations;
 - f. Professional service and audit fees.

7. Technical requirements policy

7.1 Purpose

1. To define the technical requirements that Members should adhere to.

7.2 Terms of policy

7.2.1 General

1. Members must ensure that all traffic sent over the Peering Fabric conforms to the requirements of this policy.
2. Members shall ensure that their usage of SGIX is not detrimental to Peering Fabric at all times. The term "detrimental" refers to usage which, in the reasonable opinion of the Management:
 - a. does not conform to this technical connection policy;
 - b. causes undesirable load and/or traffic patterns;
 - c. adversely affects other Members and/or the entire exchange.

7.2.2 Physical interfaces

1. Ethernet interfaces attached to SGIX ports shall be explicitly configured with duplex, speed and other configuration settings and shall not be auto-sensing.

7.2.3 MAC layer

1. Frames forwarded to SGIX ports shall have one of the following ethertypes:
 - a. 0x0800 - IPv4;
 - b. 0x0806 – ARP;
 - c. 0x86dd - IPv6;
2. Frames forwarded to an individual SGIX port shall all have the same source MAC address.
3. Use of proxy ARP on the router's interface to the Exchange is not allowed.
4. Frames forwarded to SGIX ports shall not be addressed to a multicast or broadcast MAC destination address except as follows:

- a. Broadcast ARP packets;
 - b. Multicast IPv6 Neighbour Discovery packets. This does not include Router Discovery packets.
5. Traffic for link-local protocols shall not be forwarded to SGIX ports except for the following:
- a. ARP;
 - b. IPv6 ND.
6. Link-local protocols which shall not be forwarded to SGIX ports includes but is not limited to:
- a. IRDP;
 - b. ICMP redirects;
 - c. IEEE802 Spanning Tree;
 - d. Vendor proprietary discovery protocols (e.g. CDP, EDP);
 - e. VLAN trunking protocols (e.g VTP, DTP);
 - f. Interior routing protocol broadcasts (e.g. OSPF, ISIS, IGRP, EIGRP);
 - g. BOOTP/DHCP;
 - h. PIM-SM;
 - i. PIM-DM;
 - j. DVMRP;
 - k. ICMPv6 ND-RA;
 - l. UDLD;
 - m. L2 Keepalives.

7.2.4 IP layer

1. Interfaces connected to SGIX ports shall only use IP addresses and net masks assigned to them by SGIX. In particular: IPv6 addresses (link & global scope) shall be explicitly configured and not auto-configured. IPv6 site-local addresses shall not be used.

7.2.5 Routing

1. All exchange of routes across the SGIX network shall be via BGP4+.
2. AS numbers used in BGP4+ sessions across the SGIX network may not be from ranges reserved for private use.
3. SGIX supports good engineering practice and SGIX Members are encouraged to aggregate their routes in accordance with RFC2519 "A Framework for Inter-Domain Route Aggregation".

4. IP address space assigned to SGIX peering LAN shall not be advertised to other networks without explicit permission of SGIX.
5. All routes advertised across the SGIX network shall point to the router advertising it unless an agreement has been made in advance in writing by SGIX and the two Members involved.
6. All routes to be advertised in peering sessions across SGIX shall be registered in the RIR Routing Information Service database or other public routing registry.

7.2.6 Forwarding

1. Traffic shall only be forwarded to a Member when permission has been given by the receiving Member either:
 - a. By advertising a route across the SGIX network;
 - b. or explicitly in writing.
2. Traffic shall not be routinely exchanged between two SGIX ports owned by the same Member.

8. Acceptable use policy

8.1 Purpose

1. To set out the terms for acceptable usage of the Peering Fabric.

8.2 Terms of policy

8.2.1 General

1. All Members have a responsibility to ensure that Peering Fabric is available on a fair basis to all Members, meaning that all Members shall have access to their maximum contracted port bandwidth for useful traffic unhindered by any inadvertent or deliberate act.
2. Where it is in their power to do so, Members shall take all reasonable measures, including measures that SGIX may propose, to ensure the correct functioning of the exchange, including proactively managing traffic on their own networks however and by whomever that traffic is generated.

8.2.2 Prevention of network flooding and denial-of-service attacks

1. Members are responsible to monitor their networks appropriately on a 24/7 basis and to ensure that their usage of SGIX Services is not likely to and does not cause network flooding or denial-of-service attacks.
2. To reduce the probability of non-intentional network flooding, or deliberate denial-of-service attacks, Members shall comply with all requirements of the Technical Requirements policy which specifies which kind of traffic and packet types may be forwarded to the Peering Fabric.

8.2.3 Unauthorised access or malicious attempts to compromise the SGIX network

1. Members shall take reasonable measures to prevent unauthorised access or malicious attempts to compromise the SGIX network.
2. Members shall not release information to any unauthorised party, which would assist with any attempt to compromise the SGIX network. This includes privileged confidential information provided to Members, as well as general information, not

already in the public domain, about SGIX that might be useful to this unauthorised party.

3. Violations of system or network security are prohibited. SGIX reserves the right to release the contact information of Members involved in violations of system security to other Members, in order to assist them in resolving security incidents. SGIX will also fully cooperate with law enforcement authorities in investigating suspected lawbreakers.
4. Examples of system or network security violations include, without limitation, the following:
 - a. Using SGIX services to compromise the security or tamper with system resources or accounts on the SGIX infrastructure or at any other site;
 - b. Use or distribution of tools designed for compromising security. Examples of these tools include but are not limited to password guessing programs, cracking tools or network probing tools;
 - c. Unauthorized access to, or use of data, systems or networks. This includes any attempt to probe, scan or test the vulnerability of a system or network or to breach security;
 - d. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network;
 - e. Forging of any TCP/IP packet or packet header or any part of the header information in an email or newsgroup posting;
5. SGIX reserves the right to disconnect all ports involved in malicious activities, and/or port scanning.

8.2.4 Illegal traffic

1. Where it is within its capability to do so, SGIX will assist the authorities by providing information to assist the prosecution of related offences, and may require Members to do the same.
2. Exchange of traffic that is, in the opinion of the Management, damaging or detrimental to the functioning of the SGIX, or to its Members, shall be considered to be non-compliant with this policy.

9. Joining and connection procedure

9.1 Purpose

1. To ensure that the procedure for admitting new Members and connecting them to the Peering Fabric is executed in accordance with the Policies and Procedures.
2. To ensure that the Members' usage of SGIX is not detrimental to the Peering Fabric and to prevent any adverse effects on other Members and/or the entire exchange.

9.2 Terms of procedure

9.2.1 Application for membership

1. The applicant must meet all the conditions for new applicants as detailed in the Membership Policy.
2. All applications for membership must be submitted online via the membership application form on the SGIX website.
3. Acknowledgement of the receipt of the membership form will be immediately and automatically forwarded to the email address provided by the applicant in the application form.
4. The applicant must read, understand and sign a copy of the MAA, and return a paper copy or scanned copy. The membership application form and MAA will be available for download from the SGIX website.
5. Where necessary, the applicant must make a co-location arrangement with a node operator.
6. The Management will conduct a due diligence of the applicant to verify that the above documents have been duly signed, and that the applicant complies with the conditions for new applicants set out in the Membership Policy.
7. The review will aim to conclude and inform the applicant of the outcome within five working days. During this time, the Management may request additional information from the applicant to facilitate the review process.
8. Once the Management has verified that the applicant has met the conditions for new applicants, a connection form and port purchase agreement shall be forwarded electronically to the applicant.
9. Applications for membership for Members re-applying to join SGIX shall require approval by the Board. In this case, the Management will forward the application to

the Board following verification that such applicants meet the same conditions for new applicants.

9.2.2 Connection

1. Applicants must complete a connection form and sign the port purchase agreement.
2. Upon the successful receipt of the connection form and signed port purchase agreement, SGIX will issue an invoice, requesting all relevant charges that apply for the subscribed services.
3. Upon the issuance of the invoice, the Management shall assist the new member to connect to the Peering Fabric. This may include necessary cable patching within the SGIX equipment racks.
4. The new Member shall also be required to provide sufficient information about their plans and deadlines, and coordinate with the Management to meet these timelines.
5. Every Member is responsible for the preparation of its own equipment.

9.2.3 Report setup

1. SGIX will provide the new Member with the address and log in details of the SGIX website. The Member shall be able to view statistics related to their traffic patterns and the aggregated traffic patterns of SGIX using the SGIX website.
2. The Member shall also be added to the mailing list where regular updates shall be provided by the Management.

10. Disconnection procedure (non-compliance)

10.1 Purpose

1. To detail the steps required to disconnect an existing Member from the Peering Fabric and also terminate their membership from the Company, due to non-compliance with the Policies and Procedures.

10.2 Terms of procedure

10.2.1 Reasons for disconnection

1. An existing Member is deemed to be non-compliant by violating the Policies and Procedures.
2. In the event of a breach of the policies, that, in the opinion of the Management, has the potential to seriously disrupt the Peering Fabric, the Management shall be empowered to immediately disconnect the non-compliant port. In this case:
 - a. The Management shall immediately inform the non-compliant Member;
 - b. The Management shall take all reasonable measures to ensure that this action is necessary before proceeding;
 - c. The non-compliant Member shall have the right to view documented logs of the affected ports;
 - d. Following this temporary disconnection, the Management may investigate the cause of non-compliance and may reconnect the Member, should the breach be resolved, or proceed with further investigation if the breach is not resolved within a reasonable time period.
3. In the event of a temporary disconnection, the following will occur:
 - a. The temporary disconnection will be announced to the Members;
 - b. The Member shall be disconnected from all services for the period of temporary disconnection;
 - c. The Member is not entitled to exercise any rights or privileges of membership during the period of temporary disconnection;
 - d. The Member shall not be liable to pay fees and charges to SGIX during the period of temporary disconnection, provided this period is longer than 24 hours;

10.2.2 Enquiry into forced disconnection based on non-compliance with Policies and Procedures

1. The Member shall have the right to appeal against any of the actions taken by SGIX in relation to its non-compliance.
2. The Member shall not be entitled to a refund for any fees paid before temporary disconnection.
3. As part of the notice of temporary disconnection, an enquiry meeting may be called, which will require at least one member of the Board to chair, in the attendance of:
 - a. one member of the Management;
 - b. at least one other Member who is not temporarily disconnected;
 - c. temporarily disconnected Members may attend should they wish to present their case to the meeting.
4. For each such Member separately:
 - a. The meeting shall hear the case for the Member's temporary disconnection as prepared by the Chairperson;
 - b. At the conclusion of the meeting, the Member shall either:
 - i. have its temporary disconnection extended pending resolution of the breach; or
 - ii. be reconnected to the Peering Fabric and have its membership rights reinstated; or
 - iii. have its membership terminated and removed from SGIX according to the terms of the MAA.
 - c. An outcome of termination shall also lead to disconnection of the Member's equipment from the Peering Fabric in accordance to section 2.4;
 - d. This process shall be completed within five working days.

10.2.3 Disconnection

1. Any notice on disconnection will be communicated to all Members by the Management and copied to the Board.
2. Members whose membership has been terminated in accordance with the above may reapply for membership. Any such application shall be made in accordance to the Joining and Connection Procedure.

11. Disconnection procedure (voluntary)

11.1 Purpose

1. To detail the steps required for an existing Member to voluntarily disconnect from the Peering Fabric and also terminate their membership from the Company.

11.2 Terms of procedure

11.2.1 Notification of Member's intention to disconnect

1. An existing Member has the right to voluntarily terminate membership of the Company and disconnect from SGIX. This requires one month's notice in writing.
2. In such situations, the Member shall be required to provide a notice of termination of membership in writing, with the following information as a minimum and submit to the Management via email for review:
 - a. Reasons for termination of membership;
 - b. Expected timelines for disconnection from the network;
 - c. Other requirements for disconnection.
3. This notice shall be forwarded to the Board and the Management.
4. Upon receipt, the Board will issue a membership termination statement to the Member via the Management.

11.2.2 Disconnection

1. Members whose membership has been terminated in accordance with the above may reapply for membership. However any such application shall be in accordance to the Joining and Connection Procedure.