National Information & Communications Technology Authority

GUIDELINE FOR

INTERNET SERVICE PROVIDER (ISP)

Issue: September, 2024 (Draft)

Document Reference No.:

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The National Information and Communications Technology Authority (NICTA), in accordance with Part XI-Division 4, Section 218 of the NICT Act,2009, is mandated to develop rules and guidelines relating to the ICT industry and ICT licensees in Papua New Guinea.

In order to fulfill the aforementioned requirement, NICTA developed this instrument titled “Guideline for Internet Service Providers”

This instrument provides an outline of regulatory guidelines for Internet Service Providers (as defined), covering key areas such as;

- licensing;
- general operational and service provisioning requirements;
- interconnection and data integrity;
- security measures and filtering of prohibited online content;
- consumer protection;
- including enforcement and compliance requirements; for ISPs to consider when providing internet service and other IP-based protocol service in Papua New Guinea.

1. INTRODUCTION

These regulatory guidelines aim to ensure the provision of high quality, reliable, and secure internet services to consumers and protecting consumers.

NICTA trusts that compliance with this guideline will promote confidence, reliability and enhance value of the internet and its related ICT system and at the same time employing best global approach in addressing the security threats and blocking the broadcast of prohibited online content over the internet.

This instrument shall be cited as the "Guideline for the Internet Service Providers". It specifies the minimum regulatory requirements that must be observed by parties involve in the internet service.

These guidelines apply to all ISPs providing internet services or any other IP-based ICT services in PNG.

2. DEFINITIONS

access provider – has the meaning given by section 136 of the Act
access seeker – has the meaning given by section 125 of the Act
Act – means, National Information and Communications Technology (NICT) Act, 2009,
content – means, all forms of information uniquely retrieved from or supplied to the internet,
ICT – means Information and Communication Technology,
IETF – means Internet Engineering Task Force,
IGSP – means Internet Gateway Service Provider,
IP – Internet Protocol,
IPR – Intellectual Property Rights,
ISP – means Internet Service Provider. In this guideline, "ISP" is used to mean both the access provider and the access seeker that provides internet service and other IP-based protocol service.
license – means a license granted under the NICT Act to authorize operation of the ICT service. In this guideline, license refers to an ISP license which is an Individual Application License.
NICTA – means National Information and Communication Technology Authority,
NIO – PNG National Intelligence Organization
QoS – means, Quality of Service
OOC – Office of Censorship
PNG – means the 'Independent State of Papua New Guinea'
PNG CERT – means PNG Computer Emergency Response Team (PNGCERT),
PNG IXP – means PNG Internet Exchange Point,
PoP – means Point of Presence

3. OBJECTIVES

The guidelines in this instrument aim to;

- promote end user confidence and ensuring that internet services are reasonably accessible to all people, and the internet service is supplied at performance standards to meet the needs of the public;
- to ensure that minimum quality of service parameters is implemented for compliance purpose;
- enhance cybersecurity and minimize use of services for illegal purposes and thus, building trust in ICT;
- to ensure control of prohibited online content,

- ensure protection and safety for consumers and minors
- provide transparent mechanism for complaint handling and ensures that complaints are handled in a fair and efficient manner.
- assist ISPs and the law enforcement agencies to structure their interactions in relation to cybercrime issues.

4. SCOPE

a) This Guideline apply to all ISPs providing Internet access services or any other internet protocol-based ICT services (hereinafter, “ISPs”).

b) This Guideline encourage ISPs to provide adequate quality of services to its customers in an easily comparable form, regardless of whether the ISP is an access provider or an access seeker and regardless of the technologies used to deliver the service.

c) The guidelines in this instrument does not replace, but rather provides supplements to other regulatory instruments and license conditions specified by NICTA.

d) Nothing in this Guideline is intended to prevent the ISPs from developing its own complementary or self-regulatory approaches to issues it considers important, consistent with existing legislation and policies, such as those relating to facilitating competition in the PNG economy and prohibiting anti-competitive behavior.

PART 1: GENERAL AND LICENSING REQUIREMENTS

5. GENERAL

a) A person or entity intending to provide internet services in PNG shall have to obtain an Application License from NICTA and subject to the conditions outlined in this instrument and License conditions.

b) The existing ISPs shall be subjected to the conditions in this instrument and the License conditions.

c) All ISPs shall comply with the NICTA Consumer Protection Rule, 2014.

d) ISPs shall comply with the NICT Act, OOC Act, and other prevalent laws or sector policies, rules, regulations, orders, decisions, guidelines, directives framed by the Government agencies and directives issued by the Government or NICTA from time to time.

6. LICENSING

a) NICTA anticipates and will ensure strict compliance with the Act and the “Standard and Special Conditions of Individual License Rule, 2024” by an ISP under the term of its license.

b) The ISP license is an Individual Application license, issued by NICTA.

c) NICTA may refuse an application on reasonable grounds and/or where the grant of license applied for would not be accommodated taking into account frequency spectrum, satellite regulation and market considerations. Such reasons shall be made known to the applicant.

d) Once a license is awarded, the details of the ISP will be published on NICTA registry, and is open to public viewing.

e) No limit is set upon the number of ISP licenses that may be granted by NICTA.

7. SPECTRUM OBLIGATIONS

a) ISPs that use spectrum to provide internet service shall pay all applicable fees and other charges, if any, to NICTA at a fixed price as determined by NICTA.

b) All ISPs shall use the spectrum in such a way that any harmful emission is avoided.

c) NICTA reserves the right to cancel or revoke assignment of frequency allocated to any ISPs on following grounds;

i. national security or national interest.
ii. non-compliance or violation of any license conditions.
iii. non-payment of fees or dues within the time limit specified by NICTA, and
iv. any other reasonable cause that NICTA thinks fit and proper to do so.

d) NICTA reserves the right to make any changes in the fees and charges from time to time and ISPs shall abide by this decision.

PART 2: OPERATIONAL AND SERVICE PROVISIONING REQUIREMENT

8. OPERATIONAL REQUIREMENTS

8.1 DELIVERY OF SERVICE (DoS)

a) All ISPs shall use the best technology in line with industry best practice to provide internet service to the public. They shall be bound by the terms and conditions of the license, as well as such directions or regulations of NICTA as per the provisions of the Act and/or other regulations/directives/instructions as amended or issued by NICTA.

b) Where traffic management practices are required in order for the efficient operation of internet service, the ISP shall be completely transparent about the practices that it has in place and how end user services are affected.

c) ISPs shall set up their nodes/servers within the geographical limits of the service area. They shall use internet protocol (IP) and shall meet the technical requirements of the ISPs to which they are connected. The equipment used by the ISPs shall be in conformity with the Interface/Protocol requirements as applicable.

d) ISPs shall take adequate steps to prevent harmful emissions from their system that may be hazardous to the environment, including people and property that may be injured or damaged, and shall take special care in respect of storage, usage, and disposal of batteries to be used in the installations and systems of the licensee.

e) ISPs shall refrain from causing interference with systems of other operators licensed by NICTA or other systems of government agencies in PNG, and shall comply with directions from NICTA or any other authorized agency for the prevention, cessation or mitigation of such interference.

f) ISPs are also required to take reasonable steps to ensure that the charging mechanisms used in connection with any of its facilities or services are accurate and reliable in all material aspects.

8.2 NETWORK AND CONNECTIVITY

a) ISPs shall be connected to the Internet Gateway Service (IGS). The ISP may be connected to other ISPs to get leased internet bandwidth if IGS PoP is not available at a specific and preferred location with the prior permission from NICTA.

b) ISPs shall access the international gateway in a technical and economically efficient manner either through fixed or mobile terrestrial services, or through satellite services. For ISPs accessing the gateway through satellite, conditions and other specifications pertaining to satellite regulations as determined by NICTA must be complied with.

c) ISPs shall take lease/sub-lease backhaul network services from a licensed access provider. In case of unavailability of access services, the ISP, with the prior approval of NICTA and other relevant government entities, may build its own access network for connecting the customers with their PoPs.

d) An ISP having multiple nodes or PoPs, shall demonstrate to NICTA that it is possible to monitor traffic in all routers or switches from the central monitoring center. An ISP shall inform NICTA of every change that takes place in its topology or configuration, and demonstrate that all routers or switches continue to be accessible from the central monitoring center.

e) ISPs shall not use any kind of VSAT for internet and data communication services without obtaining an Apparatus License issued by NICTA.

8.3 QUALITY OF SERVICE (QoS)

a) The quality of service over the Internet should conform to the following guidelines;
   i. Internet Engineering Task Force (IETF),
   ii. NICTA Telecommunications Quality of Service (QoS) Rule, 2022 and,
   iii. any other applicable minimum QoS standards define by NICTA.

b) ISPs shall be responsible for:
   i. maintaining the performance and quality of service standards.
   ii. maintaining the MTTR (Mean-Time-To-Restore) within the specified limits of the quality of service.
   iii. keeping a record of number of faults and rectification reports in respect of the service, which will be produced to NICTA as and when and in whatever form desired.

8.4 SERVICE AREA

a) An ISP may provide internet services in any district, province or town within PNG. The service area must be made known to NICTA before providing the service.

b) ISPs shall provide the service in the service area without any discrimination unless directed by NICTA in writing so to refuse.

9 SERVICE PROVISIONING REQUIREMENT

9.1 SUPPY OF INTERNET ACCESS SERVICE FOR RESALE

a) Access Providers shall ensure that their supply agreements include the following provisions:

   i. the right to suspend or terminate service supply in the event of any direction, decision or order from NICTA identifying the recipient of the services as being in breach of its license or any other legal requirement,

   ii. requirement that the recipient of the services provide any service-related information that the supplier of the services requires to comply with any direction, decision or order from NICTA, or any license condition or other legal requirement; and

   iii. the right to provide copies of any service supply agreement and any service-related information to NICTA or other legal authority.

9.2 SERVICE TERMINATION OR SUSPENSION

a) ISPs must include in their service agreement, clauses that permits immediate suspension or disconnection of an end-user's account and the termination of their service agreements on grounds that the end-user has breached any of the terms and conditions in that service agreement. The ISP may do so if;

   i. the ISP has provided the end user with an advance notice and an opportunity to remedy the breach;

   ii. the end user has failed to remedy the breach.

b) ISPs shall suspend the service agreements or terminate provision of internet service to end users under the agreement on grounds that the end user is engaging in illegal or improper activities. ISP shall inform relevant authority and act in accordance with the directives and rules of that particular authority.

c) An ISP that intends to cease operations or discontinue a specific service must give reasonable advance notice to all affected end users. In such cases, the ISP must take all reasonable measures to avoid any service interruption to its end users, including complying with any requirement specified by NICTA.

d) Pursuant to subsection (c) above, in any case in which an end user has made an advanced payment for services, and the ISP subsequently decides to discontinue operation or the specific service, the ISP must allocate a proportionate share of the advanced payment for refund to the end user.

PART 3: INTERCONNECTION OBLIGATIONS

10 INTERCONNECTION BETWEEN ISPs

a) Interconnection arrangements between access seekers and access providers shall be on mutually agreed terms and conditions. This includes peering interconnection arrangements and other arrangements such as transmit interconnection arrangements. In the event the parties could not settle on the terms of an interconnection agreement, the provisions of Part VI of the Act shall be taken to apply to those interconnection arrangements.

b) Both access seekers and access providers shall make every effort to ensure that sufficient bandwidth, domestically and internationally, is made available, and that access seekers lease sufficient bandwidth from access providers, to provide quality, reliable, high speed internet access to all customers at all times.

c) Direct interconnection between two separate ISPs is permitted. The interconnection shall be negotiated on fair, transparent and non-discriminatory commercial terms between ISPs. The obligation of interconnection shall be in compliance with Part VI of the Act.

11 INTERCONNECTION TO PNG EXCHANGE POINT (PNG IXP)

a) It shall be the obligation of individual ISPs to interconnect its network and/or computer system to the PNG IXP for the purpose of facilitating efficient routing and interconnection of IP transit networks within PNG.

b) It shall also, be the sole obligation of an ISP to distribute and receive routing information for local data to or from all members of the PNG IXP. The ISPs involve in peering, shall enter into separate peering agreements with other members before they can exchange traffic.

c) For interconnection to the PNG IXP, members and intending members must comply with the regulations and/or agreements that exists between the IXP Service Provider and also other laws deemed necessary.

d) An ISP that does not have a direct international connection to the internet through which an internet access is provided may be exempted in writing by NICTA from this obligation as stipulated in this guideline. The provisions of the Act, Part VI, Section 139, shall apply in this regard.

PART 4: DATA PROTECTION AND PRIVACY

12 DATA PROTECTION

a) ISPs shall take all reasonable measures to protect the end user's information from unauthorized use, disclosure and/or access.

b) IPs may collect and maintain end user information deliberately for its business purposes. The information shall be;
   i. fairly and lawfully collected and processed;
   ii. processed for limited and identified purposes;
   iii. relevant, accurate and not excessive;
   iv. kept no longer than necessary;
   v. not transferred to any other party except as permitted by any terms and conditions agreed with the end user as permitted by any permission or approval from NICTA or other Law Enforcement Agencies or as permitted and/or required by other PNG Laws and Regulations.

13 PRIVACY

a) ISPs collecting, maintaining and using or disclosing any individually identified end user information shall take all reasonable steps to ensure that information is accurate, relevant and current for the purposes for which it is to be used.

b) When accessing identified individual information, ISPs shall ensure that security assessment be done by relevant government agency before access to such information is granted for that purpose which it is to be used.

c) Pursuant to clause (b) above, licensees shall ensure compliance with the Act and the NIO Act 1984 section 38 & 39 and also other relevant PNG Laws. Compliance with such practices shall improve the national security assessment requirements and processes so that user information is protected and is used for the purpose it is intended for.

PART 5: CYBERSECURITY AND CYBERCRIME

14 CYBERSECURITY

a) ISP shall comply with PNG cyber security and cybercrime legislations or laws.

b) ISPs must protect consumers by default from known cyber-attacks and cyber threats and ensure that consumers are informed of such efforts and have the opportunity to opt out if desired.

c) The ISPs shall provide customers with minimum level of guidance on security best practices and with routes of reporting suspicious activity that are linked with PNGCERT where relevant.

d) ISPs shall employ best known security practices in their network when providing internet services. Such security practices shall cater for routing threats, email, computer, hackers, spywares, phishing and other cybersecurity threats in IP networks.

e) ISPs shall establish mechanisms for efficient monitoring and informing consumers of suspicious activity or vulnerabilities identified in their network and provide assistance to them in addressing any of the issues they come across.

f) The ISPs shall completely and totally be responsible for the security of their networks. They should also have in-place, well-outlined company policy (Code of Conduct) on security and security management of its networks, network forensics, network hardening, network penetration test, risk assessment and actions to fix problems and to prevent such problems from reoccurring. They should take all measures in respect of these activities.

15 CYBERCRIME AND ASSISTANCE TO LAW ENFORCEMENT AGENCIES

a) ISPs shall provide assistance to law enforcement agencies and government regulatory agencies to assist in preventing cybercrime and other illegal activity. Assistance includes the provision of information, upon lawful request by the Royal PNG Constabulary and other law enforcement agencies, or if required by order of a court, notwithstanding the general obligation to protect customer's privacy.

b) Upon request from law enforcement agencies, a service provider shall undertake all reasonable efforts to assist law enforcement agencies in executing the request.

c) An ISP shall prepare written procedures, which includes appropriate due diligence measures, for the processing of requests, and ensure that requests are followed up in pursuant to the agreed procedures.

PART 6: PROHIBITED ONLINE CONTENT AND FILTERING

16 PROHIBITED ONLINE CONTENT OR MATERIAL

a) A prohibited online content or material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony and/or is otherwise described by OOC's Regulations as objectional publications.

b) An ISP may not produce, reproduce, disseminate or broadcast information with the content that;

i. opposes the fundamental principles determined in the PNG Constitution;
ii. compromises State security, divulges State secrets, subverts State power or damages National unity;
iii. harms the dignity or interests of the State;
iv. incites ethnic hatred or racial discrimination or damages inter-ethic unity;
v. sabotages State religious' policy or propagates heretical teachings or feudal superstitions;
vi. disseminates rumors that undermine social order or disrupt social stability;
vii. propagates obscenity, pornography, gambling, violence, murder or fear or incites the commission of crimes;
viii. insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or
ix. includes other content prohibited by PNG laws or administrative regulations of the Censorship Board of PNG.

17 PROHIBITED CONTENT DETECTION AND NOTIFICATION

a) Prohibited online content or material shall be detected and classified using two following approaches:
   i. primarily by using integrated technology systems with ISPs' networks, which are configured and dedicated to classify and identify prohibited online content or material.
   ii. reports received from the public, competent government entities, law or any list identified by the Censorship Board and NICTA.

b) The scope of the prohibited online content shall be identified either by its URL, pattern, or digital footprint or by any technique which can be used to identify the scope of the prohibited online content without impairing unprohibited online content.

c) NICTA, shall, in its discretion notify the ISP of any website in the event the online content exists that fall under the classification of prohibited content defined by the Censorship Board or NICTA.

18 FILTERING AND BLOCKING OF PROHIBITED ONLINE CONTENT

18.1 General requirements for blocking prohibited online content

a) All ISPs shall install available technology, program or software to ensure that access to or transmittal of any prohibited online content be blocked or filtered.

b) ISPs should make genuine attempts to block sites distributing offensive and/or prohibited materials as stipulated in this guideline and also other PNG regulations relating to harmful content, which are normally administered and/or enforced by Censorship Board.

c) ISPs shall also block access to or close down any website in respect of which the ISP has been notified in writing by the OOC and or NICTA that pornographic or seditious material, or material of an offensive or defamatory nature, is being distributed from that website and where the ISP is lawfully obliged to terminate access to that website following delivery of that notice from the OOC and NICTA.

d) An ISP shall close down or block access to an internet site or sites if required in writing to do so by a law enforcement agency or by NICTA, for the reason being that the internet site(s) is reasonably suspected of being used for cybercrime or other illegal activity, for propagating computer virus or for other activities contrary to the laws of Papua New Guinea.

e) Other than in the circumstances described above, ISPs will take no action to block access to any website or internet or IP address.

18.2 Further provisions with blocking prohibited online content

a) ISPs shall block access to prohibited online content while taking the following into consideration:

   i. blocking shall not affect unprohibited content (to the extent possible).
   ii. ISPs shall block online prohibited content as defined in Part 6, section 16 and 17 of this guideline.
   iii. blocking shall not adversely affect the stability of internet network and services in PNG.

iv. blocking shall remain until it is lifted due to the removal of the prohibited online content based on an acknowledgement or report to the ISPs to confirm the content is removed or under the direct instruction of NICTA.

b) If blocking prohibited online content or material results in or can results in blocking unprohibited content, in such case ISPs shall seek guidance from NICTA where it will consider the following in reaching its decision:
   i. the scale and impact of the prohibited online content compared to the scale, impact and significance of the unprohibited content.
   ii. probability of reappearance of the prohibited online content; and,
   iii. any other factors that NICTA deems appropriate to be in the public interest.

c) An ISP who is in doubt as to whether any content would be considered prohibited may refer such content to the OOC for its decision.

d) ISPs shall inform end users with a blocking message once they attempt to access prohibited online content according to their technical capabilities and policies that they set.

e) In addition to compliance with regulations, the licensee must comply with directions or orders formally given in writing by NICTA to take down or block access to internet websites or other online content that infringes any regulations that are currently in force relating to such matters**.**

18.3 Technical remediation for filtering prohibited content and/or material.

Filtering content on the internet involves several technical measures and strategies. ISPs shall use any of the following remediation techniques to filter and manage online prohibited content;

a) DNS Filtering;
   i. Domain Name System (DNS) Blocking;
   By blocking DNS requests to specific domains known to host harmful content, ISPs can prevent users from accessing those sites. This can be implemented through blacklists of domain names or IP addresses.
   ii. DNS Sinkholing;
   Redirecting requests for blacklisted domains to a controlled IP address, often a warning page, can prevent access to malicious sites.

b) Content Inspection and Filtering;
   i. Deep Packet Inspection (DPI);
   Analysing the data within packets beyond the header to identify and filter out unwanted content. DPI can be used to detect and block specific types of content, such as malware or inappropriate material.
   ii. Keyword and Pattern Matching;
   Scanning content for specific keywords, phrases, or patterns that indicate prohibited material. This method can be applied to both text and URLs.

c) URL Filtering;
   i. Blacklist Filtering;
   Blocking access to websites that are on a predefined list of prohibited URLs. This list is maintained and updated based on various criteria, such as known sources of malware or inappropriate content.

ii. Whitelist Filtering;
Allowing access only to a predefined list of approved websites while blocking all others. This approach is more restrictive and is often used in environments requiring strict control.

d) Proxy Servers;
   i. Forward Proxies;
   Acting as an intermediary between users and the internet, forward proxies can filter content by inspecting web requests and responses. They can block or allow content based on predefined rules.
   ii. Reverse Proxies;
   Used to filter and cache content from web servers before it reaches the end user. They can also help in protecting against certain types of attacks.

PART 7: ONLINE PROTECTION OF MINORS AND OTHER VULNERABLE DEPENDANTS

19 PROTECTION OF MINORS

a) ISPs shall include in its Terms and Conditions of Service, a clear set of rules for the use of the Service that complies with the Cybercrime Act 2016, Child Online Protection Policy and all other applicable laws and regulations.

b) The Terms and Conditions shall be published prominently on the ISP's website and on all service agreements, either electronic or otherwise.

20 REPORTING CHILD SEX ABUSE CONTENT

a) An ISP shall provide clear and adequate directions to its customers for reporting child sexual abuse content to the OOC and or NICTA.

21 BLOCKING ACCESS TO CHILD SEXUAL ABUSE CONTENT

a) ISPs shall install filters to prevent receipt of material harmful to minors, provided that the filtering does not affect or interfere with access to other internet content.

b) In addition to 20 (a), an ISP shall have measures in place for the immediate blocking of access to child sexual abuse content.

PART 8: CONSUMER INFORMATION

22 PROVISIONS OF INFORMATION TO CONSUMERS

a) An ISP should ensure that their customers have access to information about potential risks to their rights-that is illegal and/or harmful content, risks for children, security and privacy online, including information on what they are doing to help their customers counter those risks.

b) The licensee shall prepare a consumer guide and make copies available to its end users and at all of its point of sale. The consumer guide must address factors expressed in the NICTA's Consumer Protection Rule, 2014 and the provisions in the Act.

c) ISPs shall furnish billing information and offerings or contracts in a form that is clear, concise, accurate and easily readable format to its customers. This information shall be published on their websites, consumer guide or on pamphlets and made readily available to their users or subscribers.

d) The licensee shall indicate clearly to the subscribers, at the time of entering into contract with such subscribers, about the specifications and the quality of their service.

23 PUBLICATION AND ADVERTISING

a) The licensee shall disclose on its website and in all service agreements, full and accurate information regarding the performance, technical and commercial terms of its internet service in a manner sufficient for customers and third-party service providers to make informed choices when intending to use their service.

b) The ISP shall also ensure that information that is retained, broadcasted and/or received through the internet shall comply with relevant provisions of the Act and the OOC's Act in-terms of Publication, Protection of State laws, Contents laws and also the laws relating to IPR and management of information on the internet.

PART 9: NATIONAL EMERGENCY SERVICES

24 EMERGENCY SERVICES

a) ISPs shall facilitate and cooperate with all relevant government bodies, departments and agencies for the continuity of traffic in the event of national emergencies or where issues of national security arise.

b) ISPs shall comply with any network or other requirements that may be approved by NICTA in terms of provision of emergency services during operation. Parameters such as location identification information, special numbers and routing for emergency service locations shall be available when providing emergency service.

c) Pursuant to clause (b) above, the following services shall be provided and easily accessed by subscribers:

i. calls free of charge for emergency services,
ii. emergency service routing localized in every province of PNG,
iii. emergency services accessible to all including persons with disabilities, and
iv. priority routing to enable consumers access emergency services.

PART 10: INSPECTION, MONITORING AND ENFORCEMENT

25 INSPECTION

a) NICTA shall audit or inspect, either directly using its own equipment and software or through independent authorities, the records relating to requirements outlined in this guideline and also other relevant instruments that NICTA has developed.

b) NICTA, if it thinks fit, may require the ISPs to get the reports audited and submitted at its own cost, through independent and qualified authorities. The inspections may be carried out with or without a representative of the licensee.

26 MONITORING

a) NICTA shall monitor and ensure compliance with this Guideline, Licensing Conditions and OOC's regulations.

b) ISP shall provide the requested information in accordance with the time-limits and the level of detail required by NICTA.

27 ENFORCEMENT

a) Whenever NICTA determines that an entity subject to the provisions of the Guideline is in breach or fails to observe the Guidelines, NICTA shall notify the entity concerned specifying the areas of non-compliance or non-observance and the specific action(s) needed to remedy the non-compliance or non-observance. The entity shall perform the action(s) specified and indicate its subsequent compliance with the Guidelines in a report submitted to NICTA within fourteen (14) working days.

b) The monitoring and enforcement of the Guidelines shall be exercised in accordance with the NICT Act. With respect to any penalties for contravention of applicable provisions, NICTA shall be guided by the considerations set out in the Act.

PART 11: COMPLAINTS

28 LODGING COMPLAINTS

a) An ISP lodging a complaint to NICTA about deteriorating of service level, interconnection and/or bandwidth from the IGSP is required to submit hard and/or soft copy evidence taken from these monitoring activities justifying their claims.

b) ISPs shall provide a mechanism that may support the customer for any questions or requests it may have regarding the service levels and general operational issues in the frame of the service covered by their service agreement, the provisions of this guideline and other regulatory instruments. Such mechanisms may take the form of phone numbers, e-mail addresses, web portals, chat systems, or any other methods that allow the customer to establish direct communications with a representative of the licensee.

c) ISPs must have in place adequate and effective procedures for receiving and responding to content related complaints including any takedown notices issued by NICTA or other government bodies.

PART 12: DOCUMENT ADMINISTRATION

29 AMMENDMENTS

a) NICTA shall administer this Instrument and make amendments or modifications to this Instrument as may appear to be necessary to prevent anomalies.

b) NICTA shall inform the industry on any such amendments to this Instrument through the relevant media sources.

30 EFFECTIVE

a) This Instrument will be in force and effective from the date endorsed by the NICTA Board and is subject to the appropriate provisions of the Act.

31 PUBLICATION AND DISTRIBUTION

a) This document is published on the NICTA website www.nicta.gov.pg for public information.

32 COMPLAINTS AND INQUIRIES

a) Complaints or inquiries maybe lodged in writing to the: Manager Consumer, PO BOX 8227, BOROKO, NCD. Phone: 325 8207, Facsimile: 3004829