Papua New Guinea

Department of Information and Communication Technology (DICT)

Government Internet Service Provider (ISP) Standard 2025

Document Control:

Document Name	PNG Government ISP Standard
Custodian	PNG Digital Government Services – Department of Information and Communications Technology
Edition	Draft 2
Approved by	PNG ICT Steering Committee
Date Approved	
Effective Date	
Next Review Date	

Table of Contents

PNG Government Internet Service Provider Standards 2025

PART 1. - PRELIMINARY.

1. NAME.

This instrument is the Government Internet Services Provider (ISP) Standards 2025.

2. COMMENCEMENT.

This instrument commences on 1st August 2024.

3. AUTHORITY.

This instrument is made under Section 64 of the ***Digital Government Act* 2022**.

4. SIMPLIFIED OUTLINE.

(1) This instrument prescribes standards and guidelines for Internet Service Provider (ISP) Standards. All Internet Service Providers (ISPs) and public bodies must comply with this instrument.

(2) This Instrument has been developed by the Department of Information and Communication Technology.

(3) Part 1 sets out Preliminary Matters.

(4) Part 2 The standards are set out in 5 parts. Part 2 contains Administrative Standards, Part 3 contains Regulatory Standards, Part 4 contains Technical Standards, and Part 5 contains Guidelines and Best Practices. Appendices are also part of this instrument

(5) Notes are included in this instrument to help understand by drawing attention to other provisions information or explanations. The notes are in small types, so that they don't disrupt the text. They do not contain statements of law

5. Definitions

In this instrument, unless the context otherwise requires:

“Cloud computing” is the on-demand availability of computing resources such as storage, servers, applications, and more over the internet. It eliminates the need for individuals and businesses to self-manage physical resources themselves, and only pay for what they use.

“Cyber Security” is the practice of protecting electronic devices, networks, and sensitive information from unauthorized access, theft, damage, or other malicious attacks.

“Data center” means a physical location that stores computing machines and their related hardware equipment.

“Data encryption” means a security method where data is converted from a readable format (plaintext) into an unreadable, encoded format (ciphertext).

“Internet Protocol (IP)” is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.

“Internet Protocol version 6 or IPv6” means communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

“Internet of Things (IoT)” is a network of physical devices, vehicles, home appliances, and other objects that are embedded with sensors, software, and network connectivity that allow them to collect and exchange data with other devices and systems over the Internet or other communication networks.

“Internet Service Provider (ISP)” is an organization or company that provides access to the internet to both personal and business customers.

“Network architecture” is the design and framework of a computer network. It includes the physical components, such as switches and routers, and the logical components, such as communication protocols and operational principles.

“Network infrastructure” refers to the hardware and software that enable network connectivity and communication between users, devices, apps, the internet, and more.

“Network security” is the protection of computer networks and their data from unauthorized access, misuse, or theft. It involves using both software and hardware technologies to create a secure infrastructure for devices, applications, users, and data.

“Service Level agreement (SLA)” is a contract between a service provider and a customer that defines the types, standards, and expectations of the services to be offered.

“Virtual Private Network (VPN)” means a service that provides you with a secure and private connection to the internet.

6. Objects of Standards and Guidelines

The object of these Standards and Guidelines are to:

(a) elevate the quality and reliability of Internet services provided to government departments, ensuring seamless communication and data transfer.

(b) establish secure security measures, safeguarding sensitive government information against cyber threats, and ensuring compliance with data protection laws.

(c) optimize network infrastructure, minimize downtime, and enhance the efficiency of government operations reliant on Internet connectivity.

(d) align with existing national ICT regulations and policies, fostering legal adherence and good governance practices.

(e) develop disaster recovery and business continuity plans, ensuring uninterrupted Internet services even in the face of unforeseen events.

(f) facilitate ongoing training and capacity-building initiatives, enabling government ICT professionals to stay abreast of emerging technologies and best practices.

7. Scope and Application

(1) These standards encompass many considerations, ranging from the selection of ISPs to the maintenance of a secure and resilient network infrastructure.

(2) They are designed to apply uniformly to all government departments across PNG, fostering consistency, transparency, and accountability in the realm of Internet connectivity.

(3) By delineating the roles and responsibilities of all stakeholders involved, these standards aim to streamline processes and enhance the overall quality of ICT services.

8. Roles and Responsibilities

(1) Department of Information & Communication Technology (DICT): serves as the custodian of these ISP standards, responsible for their development, maintenance, and enforcement. Its role includes:

(a) Drafting and updating ISP standards to reflect evolving technology and the regulatory landscape.

(b) Providing guidance and support to government departments in ISP selection and procurement.

(c) Overseeing compliance monitoring and enforcement.

(d) Collaborating with regulatory bodies to ensure alignment with national ICT policies.

(2) Government Departments: Individual government departments are accountable for adhering to the ISP standards and for:

(a) Participating in the selection and procurement process of ISPs in accordance with these standards.

(b) Implementing and maintaining network security measures as per the standards.

(c) Collaborating with ISPs and the DICT for effective service delivery.

(d) Reporting any non-compliance issues or security incidents promptly.

(3) Internet Service Providers (ISPs): play a pivotal role in delivering reliable Internet services to government departments. Their responsibilities encompass:

(a) Complying with the standards and relevant regulations.

(b) Providing transparent and competitive proposals during procurement processes.

(c) Ensuring the security and stability of their network infrastructure.

(d) Collaborating with public bodies to meet their specific ICT needs and objectives.

PART 2. - Administrative Standards

9. Overview

Standard 1 Administrative Standards

Standard. 1.1 Verification Process and Procedure

(1) An Internet Service Provider must undergo the Verification Process and Procedure to be approved and verified by the Department of Information & Communication Technology (DICT).

(2) The Verification Process and Procedure involves the following below;

(a) must have a status of a legal entity with PNG IPA.

(b) must register with PNG IPA as a Limited Company (Ltd) before operating.

(c) must be a registered taxpayer with PNG IRC.

(d) must ensure to have an operating bank account with Commercial Banks in Papua New Guinea.

(e) must ensure to have an Individual Network Gateway Services License from NICTA

(f) must ensure to have an individual Application License from NICTA

(g) must be a certified with ISO 9001 Certification Mobile Broad Band

(h) must be Security Certified with ISO 27001

(3) Public bodies must only use an Internet Service Provider (ISP) verified by DICT.

Standard 1.2 Service Level Agreements

(1) Internet Service Providers (ISPs) are recommended to provide a Service Level Agreement to public bodies or their customers.

(2) Service Level Agreements (SLAs) define the level of service expected by the public bodies from the service provider. It protects both the public bodies and the ISPs with manually agreed-upon terms, protocols, and measurable metrics that enable all parties to meet standards and function productively.

(3) This document should consider the following;

(a) clear definition of service provided

(b) roles and responsibilities of both the ISP and public bodies.

(c) duration and renewal of SLA

(d) escalation procedures for handling service disruptions and incidents

(4) The SLA must address the network performance and service level metrics provided to public bodies. It must have objectives or key performance indicators (KPI) that includes:

(a) class of service provided e.g. connection bandwidth, network maintenance and hardware.

(b) performance levels for reliability and customer support

(c) network monitoring and usage statistics

(d) process for reporting network issues

(e) schedule for response and resolutions of issues

(f) penalties for non-compliance with SLA requirements

(5) It must also specify public bodies' eligibility qualifications for service credits or prorated refunds should the ISP fail to deliver a set standard of performance as defined by the SLA.

Standard 1.3 Cost efficiency

(1) Efficiency in resource utilization is vital for government departments working within budget constraints.

(2) An ISP must consider cost-effective solutions within its SLAs that align with government objectives. This alignment will establish a fair relationship where costs are commensurate with the quality of service provided.

(3) An ISP must provide clear and accurate billing practices to public bodies by clearly outlining the pricing structures, fees, and any additional charges.

(4) This enables ISPs and public bodies to work in a transparent and cost-effective manner.

Standard 1.4 Customer support

(1) An ISP must provide excellent customer support to its customers including public bodies and stakeholders.
(2) The ISP must be able to address their issues and queries in a timely and satisfactory manner.
(3) ISP should also provide technical assistance and guidance to public bodies and educate them about the best practices and tips for using the internet services.

Standard 1.5 Collaboration and Interconnectivity

(1) An ISP must facilitate interconnectivity and seamless communication to promote efficiency and collaboration among public bodies.

(2) They must also support technologies and protocols that enable public bodies and stakeholders to exchange data and information effortlessly.

(3) Collaboration between ISPs and public bodies' entities must be crucial for achieving synergy in service delivery.

Standard 1.7 Environmental Considerations

(1) ISPs must consider environmental import of their operations, by ensuring to contribute to a greener, more sustainable future.

(2) They must adopt environmentally friendly technologies and practices, such as energy-efficient infrastructure and responsible e-waste disposal.

Standard 1.8 Incident Reporting Requirements

(1) ISPs must report any cybersecurity incidents to the relevant regulatory authorities such as the Nation Cybersecurity Center.

(2) ISPs must also notify the affected public bodies or stakeholders when identifying cybersecurity incidents.

Standard 1.9 Business Continuity and Disaster Recovery Requirements

(1) ISPs must have a business continuity and disaster recovery plan in place.

(2) This will ensure that they can continue to provide services to public bodies and stakeholders during a disaster.

Part 3 Regulatory Standards (Governance and Accountability)

10. Overview

Standard 2 Regulatory Standards

Standards 2.1 Licensing and Certification

(1) An ISP must ensure to hold licensing and certification required by regulatory authorities to operate as a service provider.

(2) The regulatory authorities are the following:

(a) National ICT Authority (NICTA)

(b) International Organizations of Standardization (ISO)

(c) National Intelligence Office (NIO)

(d) National Cybersecurity Center (NCSC)

(e) Department of Information & Communications Technology (DICT)

(3) All ISP must ensure that all licenses are kept up-to-date and renewed as required by the regulatory authorities.

Standard 2.2 Transparency

(1) All ISP must provide clear and easily accessible information about the service offerings on their websites, this includes internet speeds, service packages, and associated costs.

(2) An ISP must transparently communicate with public bodies using Service Level Agreements (SLAs).

(3) For Transparent billing practices, an ISP must provide detailed and easily understandable billing statements to public bodies or stakeholders.

(4) The ISP must regularly communicate network status, planned maintenance, and service disruptions through easily accessible channels such as websites, customer portals, or notifications to public bodies and stakeholders.

(5) ISP must transparently communicate its data privacy and security measures to its customers, especially public bodies.

(6) All ISP must maintain accessible and transparent customer support channel for public bodies support accessibility.

(7) An ISP must also regularly provide public bodies with network performance reports, including metrics on speed, reliability, and any other upgrades or optimization for network performance reports.

Standard 2.3 Compliance

(1) An ISP must establish clear policies and procedures to ensure compliance with existing National ICT policies.

(2) All ISPs must regularly review and update their policies to comply with any changes made to this instrument.

Standard 2.4 Data Privacy

(1) ISPs must align their practices with industry best practices and relevant data protection laws to safeguard government assets from cyberattacks and data breaches.

(2) They must mandate the implementation of robust security measures to protect sensitive government data and ensure the confidentiality, integrity, and availability of information.

(3) They must also ensure to inform public bodies about their privacy policies to obtain consent for the collection, processing, and storage of data.

Standard 2.4 Accessibility

(1) An ISP must ensure that its internet services are accessible to all, including individuals with disabilities.

(2) The ISP must provide accessible documentation and information about their services, policies, and procedures.

(3) All ISPs and public bodies must communicate information in multiple accessible information to ensure that individuals with diverse abilities can understand and engage with the information.

(4) ISPs must incorporate accessibility features in their technology, such as user-friendly interfaces, compatibility with screen readers, and options for adjustable text sizes and contrast ratios.

(5) ISPs must prioritize accessibility considerations in the procurement of equipment, software, and services.

(6) ISPs must provide training for their staff to raise awareness about accessibility issues and equip them with the knowledge to assist customers with disabilities effectively.

(7) ISPs must conduct regular user testing with individuals with disabilities to identify and address any barriers in their services.

(8) ISPs and public bodies must comply with relevant accessibility legislation and standards applicable in their jurisdiction.

Part 4 Technical Standards

11. Overview

Standard 3 Technical

Standard 3.1 Network Architecture and Protocols

(1) An ISP must implement a scalable and resilient network architecture that can consists of:

(a) Logical networks

(b) Physical networks

(c) Performance, reliability, and efficiency standards

(d) Security and access control standards

(e) Virtualization

(f) Software-as-a-Service

(g) Remote access

(2) The ISP must ensure to support both IPv4 and IPv6 protocols to accommodate the growing number of internet-connected devices for public bodies.

(3) The ISP must consider selecting appropriate routing protocols to efficiently manage and distribute routing information.

Standard 3.2 Network Security

(1) An ISP must protect its network and public bodies from unauthorized access, attacks, and breaches.

(2) By apply various security mechanisms such as the following;

(a) Firewalls
(b) Encryption,
(c) Authentication
(d) Authorization
(e) Accounting

(3) The ISP must consider enforcing security protocols such as

(a) TLS/SSL for encrypted communication
(b) IPsec for secure network traffic
(c) DNS Security Extensions for enhanced DNS security

(4) An ISP may consider the implementation of Intrusion Detection and Prevention Systems (IDPS) to identify and mitigate security threats.

(5) ISPs must regularly practice monitoring and updates to security measures to address emerging threats.

Note: For more information on Network Security, refer to the PNG Government Cybersecurity Standards, Guidelines and Best Practices 2023.

Standard 3.3 Access Control and Authentication Requirements

(1) An ISP must implement strong access control and authentication mechanisms as the following:

(a) multi-factor authentication

(b) role-based access control

(2) All ISPs must ensure that their networks and customer data are accessed only by authorized individuals.

Standard 3.4 Availability

(1) An ISP must ensure that its network is available and accessible to public bodies at all times.

(2) The ISP must also ensure to handle the expected and unexpected traffic and demand

(3) An ISP should also have backup and contingency plans in case of network failures or disruptions.

Standard 3.5 Speed and Bandwidth

(1) An ISP must consider implementing bandwidth management standards to efficiently allocate and control the use of network resources, preventing congestion and ensuring the fair usage

(2) All ISP must monitor and manage the network traffic and congestion, and allocate the bandwidth accordingly

(3) An ISP must provide sufficient speed and bandwidth to public bodies and stakeholders to meet their needs and expectations, and to support various applications and services on the government network

Standard 3.6 Redundancy and Failover Mechanisms

(1) An ISP is required to design its network with redundancy and high availability in mind.

(2) The ISP must consider implementing redundant links, devices, and paths, to minimize downtime and ensure continuous service delivery in the event of network failure

(3) The ISP must also consider Failover mechanisms to maintain service availability in case of disruptions.

(4) It is required for ISPs to do regular testing and validation of redundancy and failover configurations.

Standard 3.7 Quality of Service (QoS)

(1) The ISP must implement QoS mechanisms to prioritize and manage network traffic for public bodies.

(2) ISPs must deliver a stable and fast connection that meets or exceeds predefined benchmarks to maintain a high Quality of Service (QoS)

(3) This is to ensure low latency and sufficient bandwidth for critical applications used by public bodies or stakeholders.

(4) Meeting this standard guarantees that public bodies operations are not hampered by connectivity issues.

PART 5. - General Guidelines and Best Practices.

Financial and Procurement Guidelines

Budgeting and Cost Allocation

Ensuring fiscal responsibility. Standards encompass:

Budgeting procedures for allocating financial resources for ISP services.

Guidelines for cost allocation among government departments.

Transparent financial reporting to track ISP-related expenses.

B. Procurement Processes

Streamlining the procurement of ISP services. Standards include:

Detailed procurement processes and procedures.

Guidelines for conducting vendor assessments and due diligence.

Protocols for evaluating and selecting ISPs through competitive processes.

C. Vendor Selection Criteria

Selecting ISPs that meet government needs. Standards involve:

Establishing vendor selection criteria, considering factors such as technical capabilities, pricing, and service quality.

Vendor evaluation and scoring mechanisms.

Ensuring vendor compliance with regulatory and security standards.

D. Contractual Agreements

Formalizing ISP relationships. Standards encompass:

Protocols for drafting comprehensive contractual agreements.

Legal and technical terms and conditions in service contracts.

Provisions for dispute resolution and service level agreements (SLAs).

X. Environmental Considerations

A. Green ISP Practices

Promoting environmentally friendly practices in ISP operations. Standards include:

Encouragement for ISPs to adopt energy-efficient technologies and infrastructure.

Guidelines for reducing the carbon footprint of network operations.

Assessing and certifying ISPs' adherence to green practices through recognized standards and certifications.

B. Energy Efficiency

Fostering responsible energy consumption. Standards involve:

Best practices for optimizing data centers and network equipment for energy efficiency.

Monitoring and reducing energy consumption through efficient hardware and cooling solutions.

Reporting on energy consumption and efficiency improvements to demonstrate progress.

C. E-Waste Management

Ensuring responsible disposal and recycling of electronic waste. Standards include:

Guidelines for proper e-waste disposal methods and recycling procedures.

Encouragement for ISPs to actively participate in e-waste management programs.

Ensuring compliance with local e-waste regulations and promoting responsible e-waste practices among ISPs

XI. Training and Capacity Building

A. Training Needs Assessment

Identifying the knowledge and skill gaps. Standards include:

Conducting regular assessments to determine the training needs of government department staff.

Identifying areas where improved knowledge and skills would enhance ISP management.

Documenting training needs assessments for reference and planning.

B. Skill Development Programs

Empowering government staff with relevant skills. Standards encompass:

Developing skill development programs tailored to identified needs.

Providing access to training resources, both internally and externally.

Monitoring and evaluating the effectiveness of skill development initiatives.

C. Knowledge Sharing Platforms

Fostering a culture of knowledge sharing. Standards involve:

Establishing platforms and mechanisms for sharing knowledge and best practices among government departments and ISPs.

Encouraging collaboration and information exchange.

Recognizing and rewarding contributions to knowledge sharing.

VII. Security and Data Privacy

Data Protection and Privacy Compliance

Safeguarding sensitive data is paramount. Standards in this category encompass:

Compliance with data protection laws and regulations, both national and international.

Implementation of data privacy policies and practices to protect government data.

Ongoing monitoring and assessment of data protection measures.

Access Controls

Preventing unauthorized access to government systems and data. Standards include:

Implementing robust access control mechanisms to restrict access to authorized personnel.

Authentication and authorization protocols for user access.

Logging and monitoring of access attempts and user activities.

Incident Response and Reporting

Swift and effective response to security incidents. Standards involve:

Establishing an incident response plan with defined roles and responsibilities.

Protocols for identifying, containing, and mitigating security incidents.

Reporting procedures for notifying relevant authorities and stakeholders.

Regular Security Audits and Assessments

Continuous improvement of security measures. Standards encompass:

Conducting regular security audits and assessments of network infrastructure.

Evaluating security controls, vulnerabilities, and potential risks.

Implementing corrective actions based on audit findings.

Maintaining documentation of security audits and assessments.

VIII. Interconnectivity

Peering and Transit Agreements

Promoting efficient data exchange and connectivity. Standards in this category encompass:

Guidelines for establishing peering agreements with other ISPs and network providers.

Transit agreements to ensure seamless data traffic between government departments and external networks.

Ensuring equitable and cost-effective interconnection.

Cross-Government Collaboration

Fostering collaboration between government departments. Standards include:

Encouragement for government departments to share resources and services over the network.

Protocols for securely sharing data and information among agencies.

Collaboration with the Department of ICT to identify opportunities for synergy.

Disaster Recovery and Business Continuity

Preparing for unforeseen events. Standards involve:

Developing disaster recovery plans to maintain service availability during disruptions.

Business continuity strategies to ensure uninterrupted Internet services.

Regular testing and updating of disaster recovery and business continuity plans.

Interconnectivity is vital for efficient government operations. These standards provide guidance for establishing peering and transit agreements, fostering cross-government collaboration, and preparing for disaster recovery and business continuity to ensure that government departments can seamlessly communicate and share resources even in challenging circumstances.

XIII. Conclusion

PART 6. - Miscellaneous.

Part Compliance and Monitoring

12. Overview

Compliance and Monitoring

Ensuring accountability and compliance is integral to the successful implementation of these ISP standards. Follow the standards below to achieve this:

Compliance Monitoring: The DICT, in collaboration with relevant regulatory bodies, will conduct periodic compliance assessments of ISPs and government departments. This will include audits, reviews, and assessments to verify adherence to standards and regulatory requirements.
Enforcement Mechanisms: Mechanisms for addressing non-compliance will be established, outlining the consequences of violations and the steps for rectification. The DICT, in consultation with relevant authorities, will implement corrective actions and penalties, if necessary, to enforce compliance.
Reporting: Government departments and ISPs are obligated to report any incidents or concerns related to non-compliance, security breaches, or service disruptions. Reporting procedures and timelines will be outlined to ensure swift resolution and transparency.
Continuous Improvement: The standards will evolve to adapt to changing technology and security landscapes. Feedback mechanisms for government departments and ISPs will be established to provide insights for the continuous improvement of these standards.

. Appendices

Appendix 1

***For any Internet Service Provider who wishes to be part of the Government pool of ISPs, needs to have the following requirements checked accordingly:**Note: Tick the boxes in the provided checklist

Government Internet Service Provider Checklist			
Establishment			
Foreign Owned		**Partnership**	
Administrative			
IPA Registration			

CoC and TIN Certificate	
Regulatory	
NICTA Retail (ISP) Licenses	
+ Other class Licenses	
Technical	
Internal Connection Types (*to have more than one international connection type)*	
Access Connection Types **(***more than one connection-type redundancy)*	
Speed and Bandwidth *(Note to include maximum Bandwidth of the ISP)*	
Reliability and Uptime *(Reliable and smooth connection as per SLA)*	
Support Service (*Reliable Customer service 24/7 with quick response)*	
National Coverage (*Have offices or points of presence to cover major regions of the country)*	
PNG Internet Exchange Point (IXP) *(Isp needs to connect to a central point IXP to be included in Governments pool of ISPs)*	

XV. Acknowledgments

A. Appreciation for Stakeholder Contributions

XVI. Revision History

A. Document Update Log