PAPUA NEW GUINEA

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DIGITAL TRANSFORMATION OFFICER (DTO) MANUAL

GUIDE FOR COMPLIANCE WITH THE DIGITAL GOVERNMENT ACT 2022

VERSION 01 - 020525

DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY
TISA RUMA, Section 427, Hohola (Islander Drive), Waigani, National Capital District PO Box 784 Vision City,
WAIGANI, National Capital District | Email: secretary@ict.gov.pg

Introduction

The *Digital Government Act 2022* (No. 41 of 2022), certified on 19 July 2022, mandates the use of information and communication technologies (ICT) across public bodies in Papua New Guinea to enhance service delivery and governance. As a Digital Transformation Officer (DTO), you are central to this effort, as per *Section 9(1)*: "A public body shall designate a digital transformation officer for the purposes of this Act." This manual outlines your responsibilities, key processes, and compliance requirements to ensure your public body aligns with the Act, promoting efficient, secure, and citizen-centric digital governance.

Purpose: To equip DTOs with the knowledge and tools to fulfill their obligations under the Act, ensuring effective coordination with the Department of Information and Communications Technology (DICT) and adherence to national policies, standards and guidelines.

1. Your Role as a DTO

1.1 Appointment

- **Mandate:** *Section 9(1)* requires that "A public body shall designate a digital transformation officer for the purposes of this Act." Your appointment is mandatory to oversee digital transformation initiatives. **(*Refer to Annex 1: DTO appointment template*)**

- **Interim Measures:** Per *Section 9(3)*, "Where a public body does not have a digital transformation officer, the head of the public body shall nominate an officer to perform the functions of a DTO until such time a DTO has been designated." If not yet formally appointed, you may temporarily fulfill this role.

1.2 Core Responsibilities

Section 9(2) outlines your duties: "A digital transformation officer is –

(a) to co-ordinate with the DICT and digital transformation matters; and
(b) to facilitate integration and interoperability of the systems of the public body; and
(c) to facilitate delivery of digital services by the public body; and
(d) to manage the electronic data in the public body; and
(e) to provide ICT reports and feedback on a quarterly basis to the Department or as requested by the Secretary."

- **Liaison with DICT:** Act as the primary contact with DICT (*Section 9(2)(a)*).

- **Systems Integration and Interoperability:** Ensure your public body's systems connect and exchange data effectively (*Section 9(2)(b)*).

- **Digital Service Delivery:** Oversee digital service implementation (*Section 9(2)(c)*).

- **Electronic Data Management:** Manage data collection, storage, and security (*Section 9(2)(d)*).

- **Reporting:** Submit quarterly ICT reports to DICT or as requested (*Section 9(2)(e)*).

2. Compliance Obligations

2.1 Standards Adherence

- *Section 6(1)(g)* mandates DICT "to ensure public bodies comply with this Act." You must ensure your public body adheres to standards for cloud infrastructure (*Sections 25-26*), data repositories (*Section 28*), digital services (*Section 34*), and data classification (*Section 45*). Collaborate with DICT to implement these standards.

2.2 ICT Project Design Approval

- *Section 14(1)* states: "A public body shall not adopt or purchase and use an ICT Project Design unless a request is made in writing and approved by the Departmental Head." For projects requiring development budget or state-guaranteed funding (*Section 15(1)*):

  - Obtain a Certificate of Compliance from the Departmental Head (*Section 15(3)*).
  - Submit designs to the ICT Steering Committee for review (*Section 14(4)(a)* for projects ≥ K5,000,000) (*refer to Annex 2: CoC Form 1*).
  - Ensure alignment with the Digital Government Plan (*Section 15(2)*).

(*Refer to Annex 3: CoC Form 2*)

- Non-compliance risks penalties under *Section 15(6)*: "The head of a public body who fails to obtain a Certificate of Compliance… commits an offence."

2.3 Data Backup Requirements

- *Section 28(5)* requires: "A public body that stores its data by electronic means, shall… have its electronic data backed up, in the Central Electronic Data Repository… within one year on the date the Central Electronic Data Repository is established." Coordinate with DICT to meet this timeline, noting exceptions under *Section 28(6)* for international standards or practical reasons (three-year extension).

2.4 Social Media Registration

- *Section 41(2)* mandates (: "A public body shall not operate a social media account online without approval from the Secretary." You must:
  - Register accounts with DICT (*Section 41(3)*).
  - Ensure content is backed up in the Central Electronic Data Repository (*Section 41(6)*.
- Pre-existing accounts must be notified within 60 days of the Act's commencement (*Section 65(3)*).

(Refer to annex 6: Approval and registration of Social Media Accounts)

3. Working with the Public Service ICT Steering Committee

3.1 Committee Overview

- Established under *Section 11(1)*, the ICT Steering Committee includes DTOs from key departments (*Section 11(2)*). You may represent your public body (*Section 11(2)(h)*).

3.2 Your Involvement

- **Project Evaluation:** Present ICT project designs for review (*Section 12(d)*: "to evaluate ICT Project Designs of public bodies").
- **Policy Input:** Assist in identifying ICT policy gaps (*Section 12(e)*).
- **Meetings:** Attend as per *Section 13(2)*: "The ICT Steering Committee shall meet… at least once in every quarter," with a quorum of five (*Section 13(1)*). Declare conflicts of interest (*Section 13(6)*).

3.3 Project Approval Process

- *Section 14* details:
  - Submit designs for approval (*Section 14(2)*).
  - For projects ≥ K5,000,000, Committee recommendation is required (*Section 14(4)(a)*); for < K500,000, Departmental Head approves (*Section 14(4)(b)*).
  - Receive a Certificate of Compliance within 10 days (*Section 14(5)*) or rejection notice within 10 working days (*Section 14(6)*); deemed rejected if no response within 30 days (*Section 14(7)*).

4. Managing Digital Infrastructure

4.1 Government Private Network (GPN)

- *Section 22(4)*: "All public bodies must use the Government Private Network or an alternative network approved under Section 23." Coordinate its use; seek approval for alternatives (*Section 23(2)*). ***(Refer to annex 3: Request for alternate network template)***

4.2 Cloud Infrastructure

- *Section 25(3)*: "Within one year of the date of establishment of the Government Leased Cloud Infrastructure, all virtual private networks and digital services... must migrate." Apply for exceptions within 90 days (*Section 25(4)*). For Government Private Cloud, migrate within one year of commissioning (*Section 26(4)*). ***(Refer to annex 5: Request for alternate cloud template)***

4.3 National Electronic Data Bank

- *Section 27(2)*: The Bank holds the Central Electronic Data Repository and other servers. Ensure compliance with security standards (*Section 27(3)*).

4.4 Central Electronic Data Repository

- *Section 28(2)*: "The Central Electronic Data Repository shall be the official storage server to backup electronic data of public bodies." Back up data as required (*Section 28(5)*).

4.5 Secured Data Exchange Platform

- *Section 31(2)*: The platform shall "provide security for all government data stored or shared." Use it for secure data exchange and identity verification (*Section 31(3)*).

5. Delivering Digital Services

5.1 Service Accessibility

- *Section 34(1)*: "A public body may... make the service accessible as a digital service." Ensure accessibility per *Section 34(2)*, e.g., "use appropriate channels... and ensure accessibility to people with disabilities."

5.2 National E-Government Online Portal (SevisPNG)

- *Section 35(1)*: "The Department shall establish a National e-Government Online Portal." Use it for service delivery (*Section 35(2)*).

5.3 Open Data

- *Section 36(2)*: Ensure open data is "easily discoverable... machine-readable... up to date... high quality, user-friendly and free API access."

5.4 Shared Services

Section 37(7): "A public body shall not develop... a duplicate of... a declared shared service." Utilize declared services (*Section 37(4)*). ***(Refer to Annex 12: Potential Whole-of-Government Shared Services under the Digital Government Act 2022)***

5.5 Government Domain and Communication

- Use the government domain for emails (*Section 39(1)*) ***(Refer to Annex 7: Email request template)***, websites (*Section 40(1)*) ***(Refer to Annex 8: Website request template)***, and seek exceptions if needed (*Sections 39(3)* ***(Annex 9: Request for Approval to Host DNS Through an Approved Provider)***, *40(7)*). Social media requires Secretary approval (*Section 41(2)*).

5.6 Paperless Operations

- *Section 42*: Support DICT's paperless initiatives, e.g., "use of electronic forms and online or cloud storage."

6. Electronic Data Management

6.1 Data Classifications

- *Section 45(1)*: Classify data as "top-secret... confidential... open data" based on risk levels. Apply security controls (*Section 45(2)*).

6.2 Access Protocols

- *Section 47(3)*: "A person shall not access any electronic data… unless… the public body grants permission." Require written consent for personal data (*Section 47(3)(b)*).

6.3 Collection and Storage

- *Section 48(1)*: "A public body must collect and store data in electronic form." Transition as mandated (*Section 48(2)*).

6.4 System Integration

- *Section 50(1)*: "A public body must comply with the standards and specifications for electronic system integration." Ensure APIs meet requirements (*Section 50(2-3)*).

6.5 Data Sharing

- *Section 52(2)*: "When sharing electronic data, a public body must… ensure that the sharing… is done in a secured manner." Use the secured data exchange (*Section 52(3)*).

7. Cybersecurity Coordination

7.1 National Cyber Security Centre (NCSC)

- *Section 19(1)*: The NCSC shall "coordinate all efforts of national cyber security." Support its functions, e.g., reporting cyber incidents (*Section 19(1)(i)*). ***(Refer to Annex 10: NCSC Onboarding)***

8. Capacity Building

- *Section 9(4)*: "The Department shall… ensure digital skills and digital government capacity building programs are available to digital transformation officers." Participate in these programs. ***(Refer to Annex 11: Request for Participation in Digital Skills and Capacity Building Programs template)***

9. Enforcement and Penalties

- *Section 58(1)* lists offences, e.g., unauthorized data access, with penalties up to K100,000 or 10 years imprisonment. General non-compliance incurs fines up to K5,000 or 12 months imprisonment (*Section 58(3)*). Ensure compliance to avoid penalties.

10. Key Contacts and Resources

To ensure alignment with the Digital Government Act 2022 and seek necessary assistance and guidance on the detail processes, you should first submit the DTO appointment to DICT for recognition ***(Refer to annex1: DTO appointment template)***. Once the appointment is recognized, the following officers can be contacted for compliance and assistance with specific sections of the Act:

- **Jessy Sekere**: Acting Executive Manager, Digital Government & Shared Services | Coordination and Compliance, Oversighting CoC process and DTO appointments.

  Email: jessy.sekere@ict.gov.pg

- **Lizarhmarie Warike**: Acting Manager, Shared Services (oversight of Government Cloud)

  Email: lizarhmarie.warike@ict.gov.pg

- **John Pandi**: Acting Manager, Infrastructure (GPN, including Emails)

  Email: john.pandi@ict.gov.pg

- **Hamilton Vagi**: Officer-in-Charge, Cyber Security Division, oversighting whole of government Cybersecurity Centre (NCSC) and endpoint deployment.

  Email: hamilton.vagi@ict.gov.pg

- **Aizowe Otu**: Acting Manager, eSafety & SMMD (oversight of Social Media Accounts and Mis/Disinformation)

  Email: aizowe.otu@ict.gov.pg

- **Lillian Smith**: Acting Manager, Data Governance (oversight of Data Governance for whole of government)

  Email: lillian.smith@ict.gov.pg

- **Benedict Sike**: Manager, Digital Government Standards (oversight of Digital Government Standards including websites, email, etc.)

  Email: benedict.sike@ict.gov.pg

- **Joshua Pomaloh**: Acting Executive Manager, DevOps (oversight of applications and solution development and guidance on solution development)

  Email: joshua.pomaloh@ict.gov.pg

- **Jesse Biribudo**: Acting Manager, DevOps and Websites (oversight of website development and applications development)

  Email: jesse.biribudo@ict.gov.pg

- **Allan Long**: Executive Manager, Policy & M&E (oversight of policy development and alignment)

  Email: allan.long@ict.gov.pg

- **Tessie Leva:** Manager partnership, oversighting all partnerships for DICT

  Email: Tessie.leva@ict.gov.pg

By contacting these officers, you can receive the support necessary to ensure that your public body complies with the Digital Government Act 2022 and aligns with the relevant digital government policies, standards and processes.

As a DTO, you are key to implementing the *Digital Government Act 2022*. Use this manual, with its specific references, to ensure compliance and advance PNG's digital governance goals.

This DTO manual will be updated from time to time to ensure it is relevant and up to date to ensure we are aligned with the evolving nature of our sector

Authorized for release

STEVEN MATAINAHO
Secretary,
Department of ICT

DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY
Office of the Secretary
Signed:
Date:

Annex 1: DTO Appointment Template

[Official Letterhead of the Public Body]
(e.g., Department/Agency Name, Address, Contact Details)

Date: [Insert Date]

STEVEN MATAINAHO
Secretary
Department of Information and Communications Technology
P. Box 784
Vision City
WAIGANI
National Capital District

Dear Secretary,

SUBJECT: NOMINATION FOR DIGITAL TRANSFORMATION OFFICER (DTO) APPOINTMENT

In accordance with **Section 9 of the Digital Government Act 2022**, and following the **DTO appointment process**, I hereby nominate a Digital Transformation Officer (DTO) for [Name of Public Body].

Nominee Details:

- **Full Name:** [Nominee's Name]
- **Current Position:** [Position Title]
- **Contact Details:** [Email Address & Phone Number]
- **Qualifications & Relevant Experience:** [Brief Summary]
- **Justification for Nomination:** [Provide reason for selection and relevance to ICT/Digital Transformation]

Upon appointment, the nominee will:

- Coordinate with DICT on ICT and digital transformation matters.
- Facilitate system integration and interoperability.
- Support the delivery of digital services by the public body.
- Manage electronic data within the public body.
- Provide quarterly ICT reports to DICT or as requested by the Secretary.

We kindly request DICT's confirmation of this appointment. Additionally, should there be any future changes in the DTO designation due to resignation, termination, or reassignment, we will formally notify DICT.

We look forward to your confirmation and further collaboration in advancing digital transformation in Papua New Guinea.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Annex 2: CoC Form 1 - Section 14 Request

Digital Government Act 2022 (Section 14)

ICT PROJECT DESIGN REQUEST FOR APPROVAL FORM

Contact the Department of Information and Communication Technology help desk (DICT) if you have any questions about filling in this form

Details of public body making request

(All fields must be completed)

Name of Public Body

Address of Public Body

Contact details for Head of the Public Body

Contact Details for person/officer at the Public Body responsible for the request

Description of the ICT Project Design *(Provide context on what this project is about. In addition, describe the design of your ICT project type and provide relevant details.* ***Separate documentation can be attached/provided for this****).*

** This question seeks clarification of the Project's Purpose, and verification that the ICT Project Design is in alignment with Digital Government Act 2022 (It's important to attach a copy of the ICT Project Design including the architecture)*

Estimated annual cost of the ICT Project Design

What is the value of the project?

□ x < K500, 000
□ x <K500, 000 < x < K5, 000,000
□ x > K5, 000,000

** This assists DICT in approving according to Delegations of Authority*

Needs/Funding Analysis (Identify gaps, bottlenecks or pain points in existing ICT systems and operations of your organization. Specify how the proposed project will address these needs.)

** Help us understand how your project aligns with the DGA's objectives by identifying existing ICT system challenges and explaining how your project addresses these needs*

DICT COMPLIANCE HELP DESK

S Should you require assistance to complete this form or further information, please send an email to compliance team on: compliance@ict.gov.pg

Notes to Applicant

On receipt of all the required documentation for the request, DICT will respond in writing to the public body acknowledging the application. Thirty (30) days after the date of acknowledgement of the request or within such period extended by the DICT Departmental Head in writing, application will be processed.

DICT may request the public body to provide additional information for the purposes of assessing the request.

If the ICT project design is approved, a Certificate of Compliance will be issued to the public body within 10 working days after the approval decision. If the ICT project design is rejected, a written notice of rejection will be provided to the public body within 10 working days after the rejection decision.

Annex 3: CoC Form 2 - Section 15 Request

Papua New Guinea

Digital Government Act 2022 (Section 15)

REQUEST FOR CERTIFICATE OF COMPLIANCE FOR ICT PROJECT DESIGN REQUIRING DEVELOPMENT BUDGET FUNDING OR STATE GUARANTEREED FUNDING

Contact the Department of Information and Communication Technology (DICT) compliance team if you have any questions about filling in this form

Details of public body making request

(All fields must be completed)

Name of Public Body

Address of Public Body

Contact details for Head of the Public Body

Contact Details for person/officer at the Public Body responsible for the request

Description of the ICT Project Design *(Same details provided in form 1 can be copy pasted here).*

** Same copy of the ICT Project Design including the architecture requested in form 1*

Needs/Funding Analysis (*Identify gaps, bottlenecks or pain points in existing ICT systems and operations of your organization. Specify how the proposed project will address these needs.*)

** Help us understand how your project aligns with the DGA's objectives by identifying existing ICT system challenges and explaining how your project addresses these needs*

Source of Funding (Describe where the funding of this project is coming from)

** Please specify the source of project funding to help us assess eligibility for Development Budget or State guaranteed funding and understand any involvement of external donor agencies in funding your ICT project.*

Date of Request: / /2025

DICT COMPLIANCE HELP DESK

Should you require assistance to complete this form or further information, please send an email to compliance team on compliance@ict.gov.pg

Notes to Applicant:

On receipt of all the required documentation for the request, DICT will respond in writing to the public body acknowledging the application. Thirty (30) days after the date of acknowledgement of the request or within such period extended by the DICT Departmental Head in writing, application will be processed.

DICT may request the public body to provide additional information for the purposes of assessing the request.

If a Certificate of Compliance is not issued for the ICT Project Design, the public body will not be considered for development budget funding or State guaranteed funding.

Annex 4: ALTERNATE NETWORK REQUEST

[Official Letterhead of the Public Body]
(e.g., Department/Agency Name, Address, Contact Details)

Date: [Insert Date]

STEVEN MATAINAHO
Secretary
Department of Information and Communications Technology
P. Box 784
Vision City
WAIGANI
National Capital District

Dear Secretary,

SUBJECT: REQUEST FOR APPROVAL TO UTILIZE AN ALTERNATIVE NETWORK INSTEAD OF THE GOVERNMENT PRIVATE NETWORK (GPN)

In accordance with Section 22 of the Digital Government Act 2022, which mandates the establishment and utilization of the Government Private Network (GPN) for secure communications among public bodies, we hereby seek approval to utilize an alternative network tailored to our specific operational requirements.

The **[Name of Public Body]** acknowledges the critical role of the GPN in ensuring standardized and secure communications across government entities. However, due to ***[provide specific reasons, e.g., unique operational needs, existing infrastructure, specialized services***], we propose the adoption of an alternative network that aligns more closely with our objectives.

1. **Details of the Proposed Alternative Network:** [Insert provider/name e.g., Digicel MPLS, Telikom VPN, etc.]

2. **Justification for Usage (in brief):** [e.g., Enables connectivity in remote sites; supports critical systems pending GPN availability; ensures continuity of service, urgent operational requirements, lack of GPN coverage in certain areas, etc]

4. Assessment of the network provider

We have engaged with [***network provider***] to assess the feasibility and benefits of this alternative network. Their insights have been instrumental in shaping this proposal.

5. Request for Approval

Pursuant to Section 22 of the Digital Government Act 2022, we seek the Department's approval to adopt and implement this alternative network. We believe this initiative aligns with our commitment to enhancing public service delivery through innovative ICT solutions.

6. Supporting Documentation

- [*Attach any relevant documents, such as technical assessments, risk analyses, stakeholder endorsements, or compliance reports*]

We are prepared to provide any additional information or clarification as required.
Sincerely,

[Department/Agency Heads Full Name] & [Title]

Annex 5: ALTERNATIVE CLOUD PROVIDER REQUEST

[Official Letterhead of the Public Body]

(e.g., Department/Agency Name, Address, Contact Details)

Date: [Insert Date]

STEVEN MATAINAHO

Secretary
Department of Information and Communications Technology
P.O. Box 784
Vision City
WAIGANI
National Capital District

Dear Secretary,

SUBJECT: REQUEST FOR APPROVAL TO UTILIZE AN ALTERNATIVE CLOUD PROVIDER INSTEAD OF THE GOVERNMENT-SANCTIONED CLOUD/DATACENTER

In accordance with Section 25 of the *Digital Government Act 2022*, which requires public bodies to utilize the Government-sanctioned Cloud/Datacenter hosted by DICT or an approved delegate/provider, we respectfully seek approval to adopt an alternative cloud solution tailored to our operational context.

The [Name of Public Body] recognizes the importance of centralized and secure government data management. However, due to [briefly state reason—e.g., existing cloud infrastructure, latency concerns, specific compliance requirements], we propose using an alternate cloud platform to meet immediate needs while ensuring alignment with national ICT objectives.

1. **Details of the Proposed Alternative Cloud Provider (Must be one of the approved cloud service providers):** [Insert provider name – e.g., DataCo, Microsoft Azure, Amazon Web Services (AWS), Google Cloud, etc.]
2. **Justification for Usage (in brief):** [e.g., Existing environment with certified security; supports application architecture; improves service reliability, Offers specialized services not currently available through the government-sanctioned cloud]
3. **Assessment of the Cloud Provider:** We have engaged with [cloud provider] and conducted a preliminary assessment of their capabilities and alignment with security and compliance requirements.
4. **Request for Approval:** Pursuant to Section 21 of the *Digital Government Act 2022*, we kindly request DICT's approval to adopt and operate on the proposed cloud platform. We remain committed to integrating with the Government Cloud Framework when technically feasible.
5. **Supporting Documentation:** [Attach any technical evaluations, compliance checklists, service-level agreements, or internal IT assessments]

We remain available to provide further information or technical clarifications as required.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

***Noted**: Government Sanctioned cloud refers to cloud services mandated under Section 21 of the DGA.*

Annex 6: Approval & Registration to Operate a Social Media Account

[Official Letterhead of the Public Body]

Date: [Insert Date]

To:
Mr. Steven Matainaho
Secretary
Department of Information and Communications Technology
P.O. Box 784
Vision City, Waigani
National Capital District

Dear Secretary,

Subject: Request for Approval & Registration to Operate a Social Media Account

In accordance with Section 41 of the Digital Government Act 2022, which governs the operation of social media accounts by public bodies, we seek approval to establish and manage the following official social media account:

1. **Platform:** [e.g., Facebook, Twitter, LinkedIn]
2. **Account Name:** [Insert Official Account Name]
3. **Purpose:** [Briefly describe the intended use, e.g., public awareness, service updates, stakeholder engagement]
4. **Proposed Duration of Use:** [e.g., Ongoing, or specify time frame]

We are committed to adhering to the standards, guidelines, and specifications set forth by the Department for the management of official social media accounts. All content published will be considered official government information and will be backed up in the Central Electronic Data Repository, as stipulated in Section 41(6) of the Act.

Furthermore, we acknowledge that the Departmental Head is designated as the co-administrator of all public bodies' social media accounts, as per Section 41(13).

Please find attached any supporting documentation required for this application.

We appreciate your consideration of this request and look forward to your approval.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Annex 7: Request for Approval to Use an Alternative Email Domain

[Official Letterhead of the Public Body]

Date: [Insert Date]

To:
Secretary
Department of Information and Communications Technology
P.O. Box 784
Vision City
Waigani, National Capital District

Dear Secretary,

Subject: Request for Approval to Use an Alternative Email Domain

In accordance with Section 39(3) of the Digital Government Act 2022, we seek approval to use an alternative email domain for official communications due to [brief justification, e.g., ongoing integration processes, technical constraints, etc.].

Proposed Alternative Email Domain: [e.g., @abg.gov.pg]

Duration of Use: [e.g., Six months from approval date]

We assure compliance with all other provisions of the Act and will transition to the government domain as soon as practicable.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Annex 8: Request for Approval to Use an Alternative Website Domain

[Official Letterhead of the Public Body]

Date: [Insert Date]

To:
Secretary
Department of Information and Communications Technology
P.O. Box 784
Vision City
Waigani, National Capital District

Dear Secretary,

Subject: Request for Approval to Use an Alternative Website Domain

Pursuant to Section 40(7) of the Digital Government Act 2022, we request approval to operate our official website using an alternative domain due to [brief justification, e.g., existing contractual obligations, technical limitations].

Proposed Alternative Website Domain: [e.g., www.abg.gov.pg]

Duration of Use: [e.g., Until December 31, 2025]

We commit to aligning with all other requirements outlined in the Act and transitioning to the government domain within the stipulated timeframe.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Annex 9: Request for Approval to Host DNS Through an Approved Provider

[Official Letterhead of the Public Body]

Date: [Insert Date]

To:
Steven Matainaho
Secretary
Department of Information and Communications Technology
P.O. Box 784
Vision City
Waigani, National Capital District

Dear Secretary,

Subject: Request for Approval to Host DNS Through an Approved Provider

In line with the provisions of the **Digital Government Act 2022**, and in recognition of the Department's mandate to oversee and regulate government ICT infrastructure, we write to formally seek approval for the **[Insert Public Body Name]** to host our Domain Name System (DNS) services through **[Insert Name of DICT-Approved DNS Provider or "the Department"]**.

We understand and fully support the directive that all DNS services for public sector domains must be hosted by either **DICT** or a provider **formally approved by the Department** to ensure consistency, security, and reliability across government systems.

Please find our proposed arrangement below:

- **Domain(s) Involved:** [e.g., www.agency.gov.pg, mail.agency.gov.pg]
- **Preferred Hosting Provider:** [e.g., DICT, Telikom Limited, or another approved provider]
- **Justification:** [e.g., Enhanced cybersecurity and resilience, centralised management under DICT policy]
- **Duration:** [e.g., Permanent, or specify if for an interim period during migration]

We kindly request the Department's endorsement of this arrangement, or guidance on the next steps if a different configuration is recommended.

Thank you for your continued leadership in the digital transformation of government services.

Yours sincerely,

[Department/Agency Heads Full Name]
[Title]

Annex 10: National Cyber Security Centre (NCSC) – Cybersecurity Onboarding Template for Public Bodies

[Agency Letterhead]

[Date]

Mr. Steven Matainaho
Secretary
Department of Information and Communications Technology (DICT)
TISA Haus, Islander Drive
Waigani Drive, National Capital District
Port Moresby, Papua New Guinea

Dear Secretary Matainaho,

Subject: Request for Cybersecurity Onboarding with the National Cyber Security Centre (NCSC)

In alignment with Section 19(1) of the Digital Government Act 2022, which mandates the National Cyber Security Centre (NCSC) to coordinate all national cybersecurity efforts, we formally seek to initiate the onboarding process with the NCSC to enhance our agency's cybersecurity posture.

Agency Information:

- Agency Name: [Insert Agency Name]
- Department/Division: [Insert Department/Division]
- Head of Agency: [Insert Name & Title]
- Primary Contact Person (usually is the DTO):
  - Name: [Insert Name]
  - Title: [Insert Title]
  - Email: [Insert Email]
  - Phone: [Insert Phone Number]

Cybersecurity Posture Overview:

- Existing Cybersecurity Frameworks or Policies: [e.g., ISO 27001, NIST, internal policies]
- Current Cybersecurity Tools and Services in Use: [e.g., firewalls, antivirus, intrusion detection systems]
- Cybersecurity Personnel:
  - Number of dedicated cybersecurity staff: [Insert Number]
  - Roles and responsibilities: [Insert Details]

Incident Reporting:

- Have there been any cybersecurity incidents in the past 12 months?
  - ○ Yes
  - ○ No
- If yes, please provide a brief description: [Include date, nature of the incident, and response measures taken]

Engagement Objectives with NCSC:

- Incident Reporting and Management
- Threat Intelligence Sharing

- Vulnerability Assessment and Penetration Testing
- Security Awareness and Training
- Policy and Compliance Guidance
- Other (please specify): [Insert Details]

Preferred Engagement Method:

- Direct Coordination with NCSC
- Through Department of Information and Communications Technology (DICT)
- Via Third-Party Managed Security Service Provider (MSSP)
    - If MSSP, provide details:
        - Company Name: [Insert Name]
        - Contact Person: [Insert Name]
        - Services Provided: [Insert Details]

Additional Information:

- Specific Challenges or Concerns: [e.g., resource constraints, legacy systems, remote locations]
- Support Requested from NCSC: [e.g., technical assistance, policy development, training programs]
-

We believe that collaboration with the NCSC will significantly enhance our agency's ability to protect against cyber threats and ensure compliance with national cybersecurity standards.

Please advise on the next steps required to formalize this onboarding process. We are prepared to provide any additional information or documentation necessary to facilitate this engagement.

Thank you for your attention to this matter.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Submission Instructions:

Please complete this template and submit it to the NCSC via email at ncsc@ict.gov.pg. For further assistance or inquiries, contact the NCSC at the provided email address.

Note:

This onboarding process is designed to foster collaboration between public bodies and the NCSC, ensuring a unified approach to national cybersecurity efforts. By providing the requested information and onboarding, your agency contributes to the strengthening of Papua New Guinea's cyber resilience not only within your agency but across government.

Annex 11: Request for Participation in Digital Skills and Capacity Building Programs under Section 9(4) of the Digital Government Act 2022

[Agency Letterhead]

[Date]

Mr. Steven Matainaho
Secretary
Department of Information and Communications Technology (DICT)
TISA Haus, Islander Drive
Waigani Drive, National Capital District
Port Moresby, Papua New Guinea

Dear Secretary Matainaho,

Subject: Request for Participation in Digital Skills and Capacity Building Programs under Section 9(4) of the Digital Government Act 2022

In accordance with Section 9(4) of the Digital Government Act 2022, which mandates the Department of Information and Communications Technology (DICT) to develop and ensure digital skills and digital government capacity building programs are available to Digital Transformation Officers (DTOs), we formally express our interest in participating in these programs to enhance our agency's digital capabilities.

Agency Information:

- **Agency Name:** [Insert Agency Name]
- **Department/Division:** [Insert Department/Division]
- **Head of Agency:** [Insert Name & Title]
- **Primary Contact Person:**
    - Name: [Insert Name]
    - Title: [Insert Title]
    - Email: [Insert Email]
    - Phone: [Insert Phone Number]

Digital Transformation Officer (DTO) Details:

- **DTO Name:** [Insert Name]
- **Designation Date:** [Insert Date]
- **Email:** [Insert Email]
- **Phone:** [Insert Phone Number]

Capacity Building Needs:
We seek to participate in the following capacity building programs:

- Digital Skills Training
- Digital Government Framework Workshops
- ICT Policy Development Seminars
- Cybersecurity Awareness and Training
- Data Management and Governance Training

- Other (please specify): [Insert Details]

Justification:
Our agency recognizes the importance of equipping our DTO and relevant staff with the necessary skills and knowledge to effectively implement digital transformation initiatives. Participation in these programs will enable us to:

- Align with national digital government strategies
- Enhance service delivery through digital platforms
- Ensure compliance with ICT policies and standards
- Strengthen cybersecurity measures within our operations

Additional Information:

- **Specific Challenges:** [e.g., resource constraints, legacy systems, remote locations]
- **Support Requested from DICT:** [e.g., technical assistance, training materials, mentorship programs]

We kindly request DICT to provide information on the schedule, enrollment procedures, and any prerequisites for the aforementioned programs. Our agency is committed to collaborating with DICT to achieve the objectives outlined in the Digital Government Act 2022.

Thank you for your attention to this matter. We look forward to your positive response and guidance on the next steps.

Sincerely,

[Department/Agency Heads Full Name]
[Title]

Note: ***DICT will coordinate with respective public bodies as and when the potential training opportunity is available based on the requirement from the respective agencies needs***

Annex 12: Potential Whole-of-Government Shared Services to Declared under the Digital Government Act 2022

The Digital Government Act 2022 of Papua New Guinea empowers the Department of Information and Communications Technology (DICT) to establish and manage shared services that enhance the efficiency, security, and interoperability of government operations. Section 37(7) of the Act mandates that public bodies utilize declared shared services to avoid duplicative development.

The following services are identified as potential shared services to be formally declared under the Act:

1. **Whole of Government Financial management System (Integrated Financial Management System (IFMS)):** A centralized platform for managing government financial operations, including budgeting, accounting, and payment processing.
2. **Whole of Government Human Resource Management System (ALESCO Payroll System):** Standardized payroll processing and human resource management system for government employees.
3. **Government Cloud Platform (GovCloud)/Data Centre:** Secure cloud/Data Centre infrastructure for hosting government applications and services.
4. **Government Private Network (GPN):** Dedicated network ensuring secure interconnectivity among government entities.
5. **Central Electronic Data Repository (CEDR):** Centralized storage for electronic government data, ensuring redundancy and security.
6. **National Electronic Data Bank:** Physical facility housing critical government data infrastructure.
7. **Centralized Email and Collaboration Tools:** Standardized email services and collaborative platforms for government communication.
8. **Government Domain Services:** Management of official government domain (.gov.pg) names (@agency.gov.pg) and associated services.
9. **Digital Identity Management System:** Platform for managing digital identities of citizens and government employees.
10. **Secured Data Exchange Platform:** Facilitates secure data sharing among government systems and services.
11. **National Cyber Security Center (NCSC):** Monitors and responds to cybersecurity threats across government networks.
12. **Physical Security Surveillance Systems:** Digital surveillance solutions for securing government facilities.
13. **National e-Government Online Portal:** Centralized portal providing access to various government digital services.
14. **Open Data Platform (OGP):** Repository for publicly accessible government data to promote transparency.
15. **ICT Incubation Hub:** Facility supporting innovation and development of new digital government solutions.
16. **Government eSignature Platform:** Secure electronic signature solution for digital document workflows, enhancing efficiency and reducing paper-based processes.
17. **Government Asset Management System:** Centralized system for tracking and managing government assets, ensuring accountability and efficient resource utilization.

18. **National Payments System (NPS):** Comprehensive framework encompassing the movement of money through various instruments such as cash, cheques, electronic payments (including Real Time Gross Settlement and Direct Credits), and card & mobile payments. The NPS is vital for efficient, reliable, and secure transactions across the economy, reducing reliance on cash and promoting financial inclusion.

19. **Government e-Payment Gateway:** A centralized platform facilitating secure and efficient electronic payments for government services, enabling transactions between citizens, businesses, and government entities.

DICT has the prerogative to approve certain service providers who meet government standards to deliver these services on behalf of the government, as per the Digital Government Act 2022. For instance, Section 25(9) of the Act, in conjunction with NEC Decision No. 40/2024, led to the establishment of the register of Cloud Infrastructure Vendors, which includes approved providers such as DataCo PNG Limited, Digitec, AWS, Microsoft Azure, Google Cloud, Oracle, and Alibaba Cloud.

I addition, respective departments/agency's can also recommend to DICT Secretary to declare certain digital services utilized across whole of government such as ***Integrated Financial Management System (IFMS) and ALESCO Payroll System.***

Note that Shared Services are referred to services that are accessed by whole of government regardless of their status such as emails, domains, etc. There services will only be declared when they are into operational phase.

By integrating with these shared services, public bodies can enhance operational efficiency, ensure compliance with national digital strategies, and improve service delivery to the public.

Annex 13: Stakeholder Onboarding Manual for Government-to-Citizen (G2C) Services on the SevisPortal

1. Introduction

This manual outlines the structured process for onboarding public bodies onto the SevisPortal, Papua New Guinea's centralized eGovernment platform for delivering Government-to-Citizen (G2C) services. It ensures alignment with the Digital Government Act 2022 and fosters collaboration between the Department of Information and Communications Technology (DICT) and participating stakeholders to deliver efficient, citizen-centric digital services.

2. Definitions

- **Greenfield Services**: New digital services developed from scratch without pre-existing digital infrastructure.
- **Brownfield Services**: Existing services with legacy systems requiring integration into the SevisPortal.

3. Roles and Responsibilities

3.1 Department of Information and Communications Technology (DICT)

- **Project Management**: Oversee planning, coordination, and execution of the onboarding process.
- **Funding**: Cover initial development costs for services on the SevisPortal.
- **Technical Support**: Provide expertise for development, integration, and ongoing maintenance.
- **Training**: Deliver training programs (in-person and virtual) on SevisPortal usage and service management.
- **Governance**: Ensure compliance with the Digital Government Act 2022 and related policies.

3.2 Participating Stakeholders (Gov agencies, SOEs, etc)

- **Service Validation**: Review and validate "As-Is" service mappings provided by DICT.
- **Approvals**: Secure organizational leadership approvals for service blueprints and integration plans.
- **User Acceptance Testing (UAT)**: Participate in testing to confirm services meet functional and operational requirements.
- **Resource Allocation**: Provide necessary personnel and technical resources for integration and ongoing support.
- **Feedback and Improvement**: Contribute to post-deployment evaluations and continuous service enhancements.

4. Onboarding Process

The onboarding process consists of eight steps, with indicative timelines to guide planning.

Step 1: Stakeholder Identification and Engagement (1-2 weeks)

- **Action**: DICT identifies public bodies for onboarding and initiates engagement through workshops or meetings.
- **Responsibility**: DICT

Step 2: Needs Assessment and "As-Is" Service Mapping (2-4 weeks)

- **Action**: DICT conducts a detailed assessment of existing services, mapping current workflows and identifying integration needs.
- **Responsibility**: DICT

Step 3: Validation and Approval (1-2 weeks)

- **Action**: Stakeholders review and validate the "As-Is" service mappings, providing feedback and securing internal approvals.
- **Responsibility**: Stakeholders

Step 4: Blueprinting and Technical Integration Planning (3-5 weeks)

- **Greenfield Services**:

    - **Action**: DICT develops service blueprints outlining the proposed digital service design.
    - **Responsibility**: DICT (development), Stakeholders (validation and approval)

- **Brownfield Services**:
    - **Action**: DICT plans technical integration with legacy systems, addressing compatibility and data migration.
    - **Responsibility**: DICT (integration planning), Stakeholders (approval and technical support)

Step 5: Development and Testing (4-8 weeks)

- **Action**: DICT develops the services, followed by joint testing and UAT to ensure functionality and reliability.
- **Responsibility**: DICT (development and testing), Stakeholders (UAT participation)

Step 6: Training (1-2 weeks)

- **Action**: DICT delivers training sessions (in-person, virtual, or hybrid) on service management, system usage, and troubleshooting.
- **Responsibility**: DICT (training delivery), Stakeholders (participation)

Step 7: Launch Approval and Pilot Implementation (2-3 weeks)

- **Action**: Stakeholders provide final approvals, and DICT initiates a pilot phase to test services with a limited user base.
- **Responsibility**: DICT (pilot implementation), Stakeholders (approval)

Step 8: Full-Scale Deployment and Continuous Improvement (Ongoing)

- **Action**: DICT rolls out services to the public, monitors performance, and collaborates with stakeholders for iterative enhancements.
- **Responsibility**: DICT (deployment and monitoring), Stakeholders (feedback and support)

5. Compliance and Governance

All onboarding activities and services must comply with the Digital Government Act 2022 and related regulations. DICT will oversee governance, conducting regular audits and ensuring adherence to legal, security, and privacy standards.

6. Risk Management

To ensure a smooth onboarding process, the following risks and mitigation strategies are considered:

- **Legacy System Compatibility**: DICT conducts thorough compatibility assessments during Step 4.
- **Stakeholder Resistance**: Engagement workshops in Step 1 include change management strategies to build buy-in.
- **Delays**: Timelines are monitored, with contingency plans for extending critical phases if needed.
- **Resource Constraints**: Stakeholders are advised to allocate dedicated personnel early in the process.

7. Performance Metrics

Post-deployment success will be evaluated using the following key performance indicators (KPIs):

- **User Adoption Rate**: Percentage of citizens using the service within the first six months.
- **Service Uptime**: Target of 99.9% availability for SevisPortal services.
- **Citizen Satisfaction**: Measured via surveys, targeting a minimum 80% satisfaction rate.
- **Resolution Time**: Average time to resolve reported issues (target: <48 hours).

8. Conclusion

This manual serves as a comprehensive guide for DICT and stakeholders to onboard G2C services onto the SevisPortal efficiently. By fostering collaboration, ensuring compliance, and prioritizing citizen needs, the SevisPortal aims to transform public service delivery in Papua New Guinea.