



**DEPARTMENT OF INFORMATION & COMMUNICATIONS TECHNOLOGY**  
**OFFICE OF THE SECRETARY**

**CIRCULAR NO. 5/2025**

**DATE: 8TH SEPTEMBER 2025**

**TO: ALL HEADS OF PUBLIC BODIES**

**CC: HON. PETER TSIAMALILI JR  
ACTING MINISTER FOR INFORMATION AND  
COMMUNICATIONS TECHNOLOGY**

**SUBJECT: MANDATORY REASSESSMENT OF ICT SYSTEMS &  
WITHDRAWAL OF CONDITIONAL COMPLIANCE CERTIFICATES**

**1. Legal Authority**

This Circular is issued under Section 5 of the Digital Government Act 2022 ("the Act"), which mandates the Department of Information and Communications Technology (DICT), through the Secretary as Administrator of the Act, to regulate, enforce, and oversee the implementation of digital government across all public bodies.

Under Sections 14 and 15, all ICT Project Designs, procurements, and investments must obtain prior DICT approval and be issued with a Certificate of Compliance (CoC) before funding, procurement, or implementation may proceed.

**2. Withdrawal of Conditional CoCs**

Effective immediately and retroactive to 8th August 2025, all conditional CoCs previously issued are hereby revoked. This action is necessary due to persistent and widespread non-compliance with the Act, including:

- Uncoordinated ICT investments without DICT approval (Sections 14, 15).
- Siloed and incompatible systems that violate integration and interoperability requirements (Sections 31, 33, 50).
- Failure to migrate to sanctioned cloud infrastructure, the Government Private Network, and the official .gov.pg domain (Sections 22, 25, 38-40).
- Storing or processing government data outside PNG without DICT's written approval (Sections 25-26, 44).

- Failure to designate qualified Digital Transformation Officers (DTOs) by the statutory deadline (Section 9).

These failures undermine data sovereignty, national security, and the Government's whole-of-government digital transformation agenda.

### 3. Mandatory Re-Assessment Process

All public bodies are required to re-apply for CoCs by following the process below:

Deadline	Requirement	Sections
30 September 2025	Re-submit DTO Designation (Form DGA-DTO-01) and ICT System Declaration (Form DGA-SYS-01), including details of all pre-existing, ongoing, and legacy systems.	Sections 9, 14
31 October 2025	Apply for a new CoC supported by a detailed Integration & Interoperability Plan.	Sections 14, 15, 31, 50
15 October 2025 (Quarterly)	Commence DTO Quarterly Compliance Reporting on system status, cybersecurity, and integration progress.	Section 9(2)(e)
28 November 2026	Complete migration to Government-Sanctioned Infrastructure, including the GovPNG Private Network, approved cloud services, and .gov.pg domains.	Sections 22, 25, 38-40

### 4. Enforcement & Penalties

Non-compliance constitutes a criminal offence under Section 58 of the Act:

- For Individuals → Fine up to K5,000 or 12 months imprisonment, or both.
- For Corporate Entities → Fine up to K10,000.
- Unauthorized operations of ICT systems or cloud services outside DICT approval may incur penalties of up to K1,000,000 (Section 25(8)).

DICT will also enforce:

- Immediate suspension of ICT-related development budget funding and state-guaranteed loans for non-compliant entities (Section 15(5)).
- Operational restrictions, including disabling unauthorized systems and prohibiting further ICT procurements.
- Publication of a non-compliance register on the DICT website, naming agencies in breach.

### 5. Technical & Infrastructure Compliance

Public bodies must immediately comply with the GovPNG Technology Stack and register for:

- Hosting Layer → Host all data and systems on Government-Sanctioned Cloud Services (Sections 25-26).
- Communications Layer → Use the Government Private Network for secure communication (Section 22).



- Building Blocks → Integrate SevisPass, SevisDEx, and the Public Service Digital ID for all G2G and G2C verification and authentication requirements (Section 31).
- Service Layer → Streamline all G2G and G2C front-end services into the SevisPortal (Sections 33-35).
- Cybersecurity Layer → Connect all public body networks to the National Cyber Security Centre (NCSC) and the Cybersecurity Operations Centre (Sections 18-19).

For technical support, contact:

- Mr Jessy Sekere, Executive Manager – Digital Government Coordination at [jessy.sekere@ict.gov.pg](mailto:jessy.sekere@ict.gov.pg)
- Mr Benedict Sike, Manager – Digital Government Standards at [benedict.sike@ict.gov.pg](mailto:benedict.sike@ict.gov.pg)

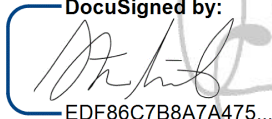
## 6. Immediate Actions Required

1. Acknowledge receipt of this Circular within seven (7) days of receiving this letter.
2. Designate your DTO and re-submit Form DGA-DTO-01.
3. Re-submit Form DGA-SYS-01, including all pre-existing, ongoing, and legacy systems.
4. Apply for a new CoC and schedule integration assessments session with DICT.

Refer to [www.ict.gov.pg](http://www.ict.gov.pg) for access to all relevant forms.

This Circular supersedes all previous directives and invalidates all previously issued CoCs. Non-compliance will trigger legal, financial, and operational enforcement under the Act.

DocuSigned by:



EDF86C7B8A7A475...

**STEVEN MATAINAHO**  
Secretary

Papua New Guinea