# THE UNITED REPUBLIC OF TANZANIA
# OFFICE OF THE SOLICITOR GENERAL

# ICT POLICY



VERSION 1.0

September, 2023

# UNITED REPUBLIC OF TANZANIA



# OFFICE OF THE SOLICITOR GENERAL

# ICT POLICY

**P.O. BOX 71554**
**10 KIVUKONI ROAD**
**11101 DAR ES SALAAM**
**TANZANIA,**
**Tel. + 255 22 2118178**

| THE UNITED REPUBLIC OF TANZANIA | | |
|---|---|---|
| Office of the Solicitor General | **Document Title** OSG ICT Policy | |
| | **Document Number** OSG/ICT/01 | |

| APPROVAL | Name | Job Title/ Role | Signature | Date |
|---|---|---|---|---|
| Approved by | Sarah D. Mwaipopo | Deputy Solicitor General | *[signature]* | Sept, 2023 |

# Definition of Key Terms

| | |
|---|---|
| OSG | Office of the Solicitor-General, conduct civil litigation, arbitration and related proceedings on behalf of the Government |
| ICT | Information and communication technologies (ICT) is defined as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information |
| INTERNET | A big network allowing communication. The internet connects smaller websites together or a global network of computers that connects them to one another |
| CONNECTIVITY | The ability to connect with other computer devices via the internet |
| DOWNLOAD | The copying of data from the internet or an online store such as games, films and music |
| PROCESSOR | The brain of the computer where everything is controlled. The speed of the processor runs on GHZ |
| HARD DRIVE | Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips |
| ISP | Internet service provider is the company that provides the internet we get to our houses |
| FIREWALL | Protect (a network or system) from unauthorized access with a firewall |

| | |
|---|---|
| LAN | A group of computers and associated devices that share a common communications line or wireless link to a server |
| WORLD WIDE WEB | Allows information to be connected to other information (Websites and webpages make up the world wide web) |
| WEBSITE(S) | A set of pages on the World Wide Web published by a single person or organisation about a particular subject or closely related topics |
| WAN | A wide-area network (WAN) is the technology that connects your offices, data centers, cloud applications, and cloud storage together |
| Desktop Computers | (also known as personal computers (PCs): designed to fit onto a desk top |
| Hardware | Computer equipment such as monitor, mouse, keyboard and CPU |

# Table of Contents

# OVERVIEW

## 1.    Background

The Office of the Solicitor General is established by Government Notice No. 50 of 2018 (the Office of Solicitor General (Establishment) Order), published in Government Gazette No. 3 Vol. 99 dated 13 February 2018. The objective of the OSG is to enhance and strengthen the Government ability to litigate civil cases, including human rights and constitutional matters in courts of law and to undertake arbitral proceedings in tribunals both in Tanzania and internationally.

The OSG is also mandated to coordinate civil litigation in all courts of law and arbitral tribunals on matters to which the Central Government, independent departments, executive agencies or local government authorities are a party or has interest. The OSG is entitled to prepare and institute suits, claims in subordinate courts, the High Court, the Court of Appeal and arbitral tribunals on behalf of the Government of the United Republic of Tanzania.

The trend towards a knowledge-based economy has emphasized the importance of ICT in development efforts in provide quality legal services to the government and facilitate access to law with an independent and impartial professionals. This shift requires a well-developed technology investment plan and intelligent deployment and maintenance management.

For OSG to realize the value out of ICT investment, ICT must be deployed to improve efficiency and effectiveness in internal and external services delivery. This means that, a comprehensive framework established by ICT Policy to provide appropriate directives to harness ICT, is necessary for achievement of OSG's objectives.

Document Number: OSG/ICT/01   Version: 1.0          Owner: Office of the Solicitor General
Title: ICT Policy

Establishment of ICT Policy is the important step toward ensuring that ICT will assist OSG to attain its objectives. The ICT Policy will ensure that the ICT infrastructure and capacity are utilized effectively and are in alignment with the OSG's strategic objectives, National ICT Policy, National e-Government Strategy and the e-Government Standards and Guidelines.

## 1.1. Mission and Vision

### Vision
To be the Best public law office leading the Government in litigation.

### Mission

To conduct civil litigation, arbitration and related proceedings efficiently and professionally on behalf of the Government

## 1.2. Mandate Role of OSG

The objectives of establishing the OSG are set out in Clause 3 of Government Notes No. 50 of 2018 as follows:

(a) To enhance and strengthen the Government ability to litigate civil cases including human rights and constitutional matters in courts of law and undertake arbitral proceedings in tribunals;

(b) To enhance effective supervision of civil cases in courts of law including human rights and constitutional matters; and

(c) To carry out the general coordination of the conduct of civil litigation and arbitral proceedings on behalf of the Central Government, independent departments, executive agencies and local government authorities.

## 1.3. ICT Service of OSG

Through the Unit, which is responsible for ICT, OSG, offers a number of ICT services to internal and external stakeholders. Internal services are those geared to support business processes of the OSG. They include mailing; Website, System support; resources management such as finance, procurement and Human resources; centralized storage; Internet; e-library; conference support; video conference; CCTV Camera management; Printing and scanning; biometric finger print management; Local Area Network; and a number of other emerging services.

Also the OSG use Ministerial Systems such as Mfumo wa Ulipaji Serikalini (MUSE), Human Capital Management Information System (HCMIS), Government e-Office System, Tanzanian National e-Procurement System (NeST); Travelling Permit System (e-Vibali); Centralized Budget Management System (CBMS) and Government Communication Network (GOVNET) so as to achieve its objective.

## 1.4. SWOC Analysis

### 1.4.1. Strength

(i)   Top management's commitment on using ICT to support the business operations.

(ii)  The presence of a large proportion on average to advanced ICT users.

(iii) The existence of the long term Business Strategic Plan of the Institute that acknowledges the contribution of ICT.

(iv)  Presence of number of e-Governance (number of computers and printers connected to internet).

(v)   Presence of Government Communication Network (GOVNET).

      (vi)   Easy access to online reference.

### 1.4.2. Weakness
      (i)     Inadequate of specialised skills in ICT.
      (ii)    Lack of a clearly established ICT Governance structure.
      (iii)   Ageing of LAN.
      (iv)   Inadequate of strong internet services to some Regional Offices
      (v)    Low level of ICT and cyber security awareness.
      (vi)   Lack of a functioning disaster recovery plan.

### 1.4.3. Opportunities
      (i)     The increased demand for ICT services among stakeholders.
      (ii)    Presence of ICT Unit and budget that support business operations.
      (iii)   The increase number of employees who have knowledge of using computer
      (iv)   The existence of e-Governance.
      (v)    The Presence of System that help core business process of the Institution.

### 1.4.4. Challenges
      (i)     Inadequate number of knowledge staff on the use of ICT infrastructure.

      (ii)    Inadequate qualified ICT staff on some specialised areas.

      (iii)   Aging in LAN.

(iv)     Presence of malicious ICT users and other cyber threats.

## 1.5.  Rationale

OSG needs to meet its objective of improving its services and increasing productivity by leveraging on new technologies. OSG has been investing in ICT to facilitate its internal business operations so as to attain its strategic goals. OSG operations are increasingly depending on ICT, making the Institution vulnerable to ICT related risks. In this regard, it is evident that, Office of the Solicitor General needs to develop and operationalize comprehensive ICT Policy to direct ICT adoption and usage within the Institution.

## 1.6.  Purpose

This document provides the highest level ICT directives for OSG. The main purpose of this document is to ensure that OSG's ICT related investment, operations and maintenance processes and usage are well directed. The specific objectives of this policy are to ensure;

(i)     ICT governance is integral part of the institutional governance;
(ii)     ICT services provisions are in line with OSG's business requirements based on existing e-Government standards and best practices;
(iii)    All OSG information resources and services are well secured using appropriate controls; and
(iv)    The members of the Institution use ICT facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.

## 1.7.  Scope

This policy is applicable to all OSG's staff and its associates, all users of ICT equipment owned or leased by the Institution as well as all equipment connected to OSG's ICT related infrastructure. This policy applies to all OSG's ICT related resources and services.

### 2.1. ICT Governance

ICT Governance is an integral part of corporate governance and consists of the leadership, organisational structures and processes that ensure that the organisation's ICT sustains and extends the organisation's strategies and objectives.

The general objective of ICT Governance is to put the strategic and operational management of ICT within the principles of ICT Governance and within the context of OSG strategic directions. Specific objectives are:

(i) Establishing a framework for ICT investment decisions, accountability, monitoring and evaluation; and

(ii) Ensuring there is formal ICT governance process that is consistent across the enterprise and has strong accountability.

#### 2.1.1. ICT Processes and Organisation

2.1.1.1. OSG will set up an ICT governance model so that it have the right structure to manage ICT operations and a secure ICT environment that complies with e-Government standards.

2.1.1.2. There shall be an ICT Steering Committee (or equivalent) to determine prioritisation of ICT-enabled investment programmes in line with the Institution's business strategy and priorities, track status of ICT initiatives, resolve resource conflicts and monitor ICT services.

2.1.1.3. OSG shall establish a strong ICT Unit capable of supporting strategic objectives of

the institution.

2.1.1.4. OSG shall ensure that ICT strategic plan and Enterprise Architecture are established and operationalized.

2.1.1.5. OSG shall ensure that ICT plans fit the current and on-going needs of OSG and that the ICT plans support OSG strategic plans.

2.1.1.6. OSG shall ensure that ICT Risk Management annually done, where ICT risk assessment is conducted and reviewed, likelihood and occurrence identified, mitigation strategy established and risks treated, accepted, transferred or avoided.

### 2.1.2. Roles and Responsibilities for ICT

2.1.2.1. OSG shall ensure that individuals and groups within the Institution understand and accept their responsibilities for ICT.

2.1.2.2. OSG shall ensure that clear and well understood contracts exist for external suppliers.

2.1.2.3. OSG shall ensure that acceptable use and related policy are known and adhered to by staff.

### 2.1.3. ICT Resources Management

2.1.3.1. OSG shall define a set of policies for ICT security, which shall be approved by management, published and communicated to employees and relevant stakeholders.

2.1.3.2. OSG shall ensure that ICT acquisitions

are made for approved reasons in an approved way; on the basis of appropriate and on-going analysis.

2.1.3.3. OSG shall ensure that there is appropriate balance between costs, risks, long-term and short-term benefits.

## 2.1.4. ICT Performance Management

2.1.4.1. OSG shall ensure that ICT is fit for its purpose in supporting the Institution, is kept responsive to changing business requirements.

2.1.4.2. OSG shall ensure that ICT Services are defined, e.g. Email services, Printing services.

2.1.4.3. OSG shall establish mechanism for evaluating and monitoring ICT services such as Service availability, staff satisfaction / feedback system

## 2.1.5. Conformance

2.1.5.1. OSG shall ensure that ICT conforms to e-Government standards and guidelines and all external regulations and complies with all internal policy, procedures and practices.

2.1.5.2. All employees and third parties have a personal obligation to comply with internal ICT policy, guidelines and procedures and must keep abreast of, and comply with, any changes. Failure to comply may result in legal or disciplinary actions.

### 2.1.6. ICT Projects Management

2.1.6.1.   OSG shall ensure that ICT conforms to the Government ICT projects management procedures and complies with all internal developed procedures for managing projects.

2.1.6.2.   OSG management team will monitor the key ICT projects undertaken and provide regular progress reports on risks identified and preventive/detective actions taken.

### 2.1.7. Procurement of ICT Equipment and Services

2.1.7.1.   OSG management will implement the necessary controls to ensure that all ICT procurements are done in line with requirements of Public Procurement Act (PPA)

2.1.7.2.   User Departments shall establish and submit, in writing, all ICT related requirements weather ad-hoc or planned, to ICT unit who will process and submit them to procurement unit.

2.1.7.3.   ICT unit shall ensure that all requirements for ICT procurements comply with e-Government Standards and Guidelines.

2.1.7.4.   Procurement unit shall not procure any ICT System, Service, Equipment, Consumable or Accessory if the request is not originating from ICT unit.

## 2.2. ICT Infrastructure

ICT infrastructure is the backbone for supporting the OSG business operations by enabling information exchange and providing secure access to different applications. This consists of all hardware devices such as network devices, servers, workstations, laptop, storage, back-up, operating facilities and supporting platform like operating systems and databases.

The objective managing ICT Infrastructure is to ensure that the OSG's ICT infrastructure operations are optimized in order to deliver higher level service quality and support business-relevant operations based on ICT planning and management best practices.

### 2.2.1. Infrastructure Planning and Design

2.2.1.1.  OSG shall ensure that ICT infrastructure architecture is in place and in line with the Institution's current and future requirements.

2.2.1.2.  OSG shall ensure that appropriate ICT infrastructure is setup and well managed.

### 2.2.2. Data Management and Storage

2.2.2.1.  OSG shall ensure that all business related data shall be stored in a way to facilitate back up procedures and access.

### 2.2.3. ICT Equipment and Hosting

2.2.3.1.  OSG shall acquire desktop computers, laptop, servers printers and networking equipment from authorized suppliers.

2.2.3.2.  All ICT resources shall be acquired in consultation with ICT unit.

2.2.3.3.  OSG shall ensure that appropriate environment for hosting computing and

storage equipment based on standards and best practices is established.

### 2.2.4. Infrastructure Maintenance and Support

2.2.4.1.　OSG shall ensure that all ICT infrastructure components are maintained at a reasonable operational and secure level.

2.2.4.2.　OSG shall ensure that standard software list including the operating system to be installed into the Institution's equipment is established.

2.2.4.3.　OSG shall procure maintenance services from organization that have technical capabilities.

2.2.4.4.　OSG shall ensure that maintenance services are procured in consultation with ICT unit.

## 2.3. Applications

Applications are software designed for end-users to use in their daily operations to support the enterprise business processes.

The general objective of managing applications is to ensure that ICT applications that are in use or are to be acquired to address the business requirements of the Public Institution and provide reasonable return on investment.

Specific objectives are:
  (i)   To ensure system acquired follow proper procedures;
  (ii)  To establish controls for efficient acquisition and administration of applications; and
  (iii) To enhance accountability on the management and usage of ICT Applications.

### 2.3.1. Applications Acquisition and Deployment

2.3.1.1.    There shall be clear understandable business and system requirements before any application acquisition.

2.3.1.2.    User departments shall submit to ICT unit their ICT requirements to be included in ICT resource budget.

2.3.1.3.    All applications supplied shall be checked by ICT unit to verify the technical if requirements established are met and approved.

2.3.1.4.    ICT unit shall establish appropriate software standards to facilitate acquisition/development.

2.3.1.5.    ICT unit shall ensure the best configuration is adopted for the system acquired.

### 2.3.2. Applications Maintenance and Support

2.3.2.1.    Administration and maintenance of applications shall be an on-going process that will last throughout the life cycle of the application.

2.3.2.2.    Every application acquired by OSG shall have documentation in place and updated regularly.

2.3.2.3.    Installation of additional applications or overriding existing one shall follow change management procedures.

2.3.2.4.    Software acquired for installation into OSG equipment shall be licensed.

## 2.4. ICT Service Management

ICT Service management deals with how ICT resources and core business practices altogether are delivered in such a way that the end user experiences the most desired results from accessing the entire solution stack.

The objectives of ICT Service Management are:

(i)   To improve internal and external stakeholder's satisfaction.

(ii)  To assist in defining meaningful metrics to measure service results and using the metrics to drive continuous service improvement.

(iii) To enable the monitoring and improvement of service quality through the effective application of processes.

(iv)  To ensure compliance with all e-Government Standards and Guidelines relating to the ICT Service Management.

### 2.4.1.   ICT Service Desk

2.4.1.1. OSG shall operate an ICT service and support function which will ensure that business disruptions are minimised, users' queries are responded to and ICT problems are resolved. An ICT Service Management document shall be developed accordingly.

### 2.4.2.   Management of Service Levels

2.4.2.1. OSG shall ensure that for every ICT services provided, Service Level Agreements between the providers and the recipients are established.

2.4.2.2. OSG shall ensure that reports on service quality are reviewed annually with

customers along in order to determine things that could be added or changed to improve service delivery and support.

### 2.4.3.  Management of Third Party Services

2.4.3.1.  OSG shall ensure proper processes and procedures for managing vendors are in place.

2.4.3.2.  OSG shall ensure that services procured from third parties (suppliers, vendors and partners) meet business requirements.

2.4.3.3.  OSG shall ensure that it builds good relationships with the business and third party providers to ensure that ICT services delivered continue to meet evolving Institution's business needs.

### 2.4.4.  ICT Service Requests, Incidents and Problems Management

2.4.4.1.  OSG shall set up a single point of contact i.e. service desk for end users where requests will be recorded, escalated to the correct group, resolved and closed to ensure restoration of normal service operations as quickly as possible.

2.4.4.2.  OSG shall ensure that ICT service catalogue is prepared and approved.

2.4.4.3.  OSG shall ensure that Service Requests and Incidents Management processes and procedures are established to ensure minimal adverse impacts on customers.

2.4.4.4.  OSG management shall review all reports about problems that resulted to systems downtime in order to identify root causes

of problems.

### 2.4.5. Change Management

2.4.5.1. OSG shall ensure that a process for recording, assessing and authorizing all changes prior to implementation, including changes on procedures, processes, systems and service parameters are established.

### 2.4.6. ICT Service Availability

2.4.6.1. OSG shall implement an availability management process to ensure that services are available, when needed, and as defined in approved Service Level Agreements.

### 2.4.7. ICT Service Continuity

2.4.7.1. OSG shall conduct a Business Impact Analysis to identify critical Business functions to be supported by ICT.

2.4.7.2. OSG shall ensure that a robust business continuity and service recovery plans are in place and that these plans are regularly reviewed and tested and key staff are appropriately trained.

### 2.4.8. Configuration Management

2.4.8.1. All information regarding ICT assets, Service Level Agreements, End User documentations version control and change requests shall be loaded into the configuration management system.

### 2.4.9. Capacity Management

2.4.9.1. OSG shall establish a capacity plan to monitor ICT resources usage for existing

and planned systems in order to assist in time and cost effective purchase of additional resources so as to avoid panic purchase when resources run out.

### 2.4.10. Data Management

2.4.10.1. OSG's business requirements for data management shall be determined and data shall conform to the Government data and metadata standards.

2.4.10.2. OSG shall develop procedures for effective and efficient data storage, retention and archiving to meet business objectives, the Institution's ICT Security Policy and regulatory requirements.

## 2.5. ICT Security

ICT Security covers all the processes by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction throughout an organization.

The general objective of managing ICT Security is to provide OSG with information security mechanism to support the Institution to achieve its strategic goals based on best practices. The specific objectives are:

(i)   Protection of the OSG's ICT resources from accidental or malicious act while preserving the open information sharing requirements of the Government; and

(ii)  Making the OSG's stakeholders aware of their responsibilities with respect of ICT security.

### 2.5.1. ICT Security Management

2.5.1.1. OSG    shall    actively    support    ICT

security within the Institution through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of ICT security responsibilities.

2.5.1.2.  OSG shall ensure information systems are designed, acquired and implemented with effective ICT security controls to safeguard the integrity, confidentiality and continual availability throughout the entire life cycle.

2.5.1.3.  ICT security Policy shall be established to highlighting the implemented ICT security controls that ensures ICT security risks are mitigated and controlled. The document may be complemented by other ICT security sub-documents that define more specific security policies for individual components of the ICT environment.

2.5.1.4.  All users of OSG systems shall be responsible for protecting Office of the Solicitor General's information resources.

2.5.1.5.  OSG shall retain overall responsibility and ownership for all Office of the Solicitor General's information assets.

**2.5.2.  Monitoring**

2.5.2.1.  OSG will monitor use of its ICT facilities and premises. This includes, but is not restricted to, accessing and reviewing the contents of servers, email accounts, hard drives, the internal telephone system, biometric attendance system,

video conference facilities access control logs and CCTV recordings (which will be installed). This is to ensure that the institution's business interests are protected, for quality control purposes, to detect abuse of the systems, or to detect or prevent crime or misconduct

### 2.5.3. Continuity Management

2.5.3.1. OSG will maintain its ICT environment so that it remains in a running state and does not affect the business performance or services. A disaster recovery plan will be developed accordingly.

# 3. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

## 3.1. Implementation and Reviews

**3.1.1.** This document shall come into operation once tabled and agreed in management meeting, and approved by Accounting Officer in its second page, and then shall be considered mandatory for all OSG business operations.

**3.1.2.** The policies described below provide top level issues for common understanding of adoption and usage at the Institution based on e-Government standards and guidelines and where necessary detail procedures could be developed.

**3.1.3.** OSG management will use this policy in conjunction with the documents in Section 5, below to ensure that it operated within a well geared ICT ecosystem.

**3.1.4.** All employees and other authorised users of OSG shall comply with requirements of this policy.

**3.1.5.** The head responsible for ICT shall enforce compliance by using audit trails and triggering access denial to OSG systems and networks.

**3.1.6.** OSG staff found to have violated this policy may be subject to disciplinary action in accordance with rules, regulation and procedures defined by Government.

**3.1.7.** This document shall be reviewed after three years, or whenever business environment of OSG changes in a way that affects the implementation of the policy.

## 3.2. Exceptions

**3.2.1.** In case of any exceptions to this policy, it shall be thoroughly documented and follow through a proper channel of authorization using the same authority which approved this document.

## 3.3. Roles and Responsibilities

### 3.3.1. Accounting officer,

3.3.1.1. Review and approve ICT Policy, and provide strategic directives on utilisation of ICT in order to enhance productivity by ensuring effective and efficient systems;

3.3.1.2. Appoint an ICT Steering Committee (or equivalent) and determine its terms of reference [Could be the Management Team Sitting with a focus on ICT Matters]; and

3.3.1.3. Ensure implementation of the ICT Policy.

### 3.3.2. ICT Steering Committee

3.3.2.1. Shall propose OSG's ICT Policy for the consideration of Accounting officer,

3.3.2.2. Shall coordinate the establishment and continues review of OSG's ICT Policy, ICT Strategy and Enterprise Architecture;

3.3.2.3. Shall ensure that the ICT Strategy is aligned with OSG's Corporate Plan;

3.3.2.4. Shall advice the Accounting officer, in making considered decisions about the focus of ICT resources;

3.3.2.5.　Shall review all ICT services and applications including Office of the Solicitor General's website and infrastructure with the view to advice Office of the Solicitor General on required improvements; and

3.3.2.6.　Shall ensure that risks associated with ICT are managed appropriately.

**3.3.3.　Directors and Head of Units**

3.3.3.1.　Shall ensure that all users under their supervision are aware and comply with this policy;

3.3.3.2.　Shall provide adequate and appropriate protection of ICT assets and resources under their control;

3.3.3.3.　Shall ensure availability, integrity and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations; and

3.3.3.4.　Shall review and approve procedures, standards, policies and guidelines developed from this policy for the purpose of maintaining business continuity and security of OSG's ICT resources.

3.3.3.5.　Shall be custodian of "Data and Information" for their respective Departments/Units.

**3.3.4. Head of ICT Unit**

Subject to general oversight of Accounting Officer, and advice of the ICT Steering Committee, the Head responsible for ICT shall oversee the overall implementation of this policy; and in particular he/she shall

3.3.4.1. Coordinate the review and amendment of this policy, as and when required in order to accommodate new technologies or services, applications, procedures and perceived dangers;

3.3.4.2. Plan and develop ICT Strategy and OSG's Enterprise Architecture and ensure its implementation.

3.3.4.3. Monitor adherence to the ICT Policy and the presence of potential threats and risks by ensuring periodic ICT security reviews are conducted

3.3.4.4. Keep abreast of ICT developments in respect of ICT industry in general and OSG's systems in particular.

3.3.4.5. Initiate and recommend proposals to change, modify or improve this policy; and

3.3.4.6. Recommend procedures, standards and rules for effective implementation of this policy in line with e-Government Standards and Guidelines.

3.3.4.7. Be the custodian of all ICT resources of OSG including those centrally stored in server room/data centre.

### 3.3.5. Head of Internal Audit Unit

3.3.5.1. Shall audit the ICT Function of OSG and ensure compliance with the policy

### 3.3.6. Users of ICT Systems

3.3.6.1. Shall be responsible to safeguard ICT assets of OSG in their custody.

3.3.6.2.

3.3.6.3.    Shall comply with this policy.

## 3.4.    Monitoring and Evaluation

**3.4.1.** ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against OSG ICT Policy, Strategic Plan and Enterprise Architecture.

# 4. GLOSSARY AND ACRONYMS

## 4.1. Glossary

**ICT Policy** – A document that elaborate on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the entire ICT Management Framework, commonly known as ICT Policy of an Institution.

## 4.2. Acronyms

- **CCTV –** Closed Circuit Television
- **ICT** **–** Information & Communication Technology
- **OSG** **–** Office of the Solicitor General

# 5.    RELATED DOCUMENTS

5.1.    ICT Policy
5.2.    ICT Strategy
5.3.    Enterprise Architecture
5.4.    ICT Security Policy
5.5.    ICT Service Management Guidelines
5.6.    Disaster Recovery Plan
5.7.    ICT Project Management Guidelines
5.8.    ICT Acquisition, Development and Maintenance Guidelines

# 6. DOCUMENT CONTROL

| VERSION | NAME | COMMENT | DATE |
|---------|------|---------|------|
| Ver. 1.0 | AZIZ MAKABURI | INITIAL DEVELOPMENT OF THE POLICY | JUNE, 2023 |

Policy Name: **OSG ICT Policy**
Policy Reference: **OSG/ICT/01**
Policy Version: **1.0**
Policy Effective Date: **September 2023**
Policy Creation: Office of the Solicitor General
Policy Changes: **Every three years**