


ICT POLICY

Version: 1.0

Authorization

Name	Job Title/Role	Signature	Date
A.Lesley Jesurajan	Chairperson, OPEnE		28 th December 2022

1.0 Purpose

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

- To ensure ICT governance is an integral part of Organizational governance.
- ICT services provisions are in line with OPEnE's business requirements based on Organization standards and best practices.
- All the Organization's information resources and services are well-secured using appropriate controls.
- To ensure the members of the organization 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.
- The purpose of the ICT Policy is to provide OPEnE with comprehensive protection against loss or Stealing of data, computer viruses, and malicious code.
- This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, and hardware
- to protect the information on individual workstations and servers, and anti-virus software protects the network. The availability, performance, and security of the network are essential to the daily operation of the Organization. Viruses and other forms of malicious code (worms, Trojans, backdoors, VBS scripts, mass mailers, etc.) represent a significant threat to this operation.
- This policy document directs the organization to establish access authorization and modification procedures to control user access to Information and Communication Technology (ICT) resources, which contain sensitive data.
- This policy document outlines acceptable use, security requirements, and confidentiality issues related to portable computers and mobile devices among all employees of OPEnE and connected and supported sites. The term portable computer and mobile device is used in this document to include: Notebooks, laptops, mini-notebooks, PDAs, Smartphones, and tablet PCs.
- This policy establishes guidelines and minimum requirements governing the acceptable use of, access to, and disclosure of the organization-provided internet/e-mail service.

2.0 Scope

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

3.0 ICT Resources Management

- OPEnE shall define a set of policies for ICT security, which shall be approved by Board, published, and communicated to employees and relevant external parties.
- OPEnE shall ensure that ICT acquisitions are made for approved reasons in an approved way; on the basis of appropriate and ongoing analysis.
- OPEnE shall ensure an appropriate balance between costs, risks, and long-term and short-term benefits.

4.0 ICT Performance Management

- OPEnE shall ensure that ICT is fit for its purpose in supporting the organization, and is kept responsive to changing business requirements.
- OPEnE shall ensure that ICT Services are defined, e.g. Email services, Printing services.
- OPEnE shall establish mechanisms for evaluating and monitoring ICT services (E.g. Service availability, staff satisfaction/feedback system).

5.0 Conformance

- OPEnE shall ensure that ICT conforms to standards software crime act policy and guidelines and all external regulations and complies with all internal policies, procedures, and practices.
- All employees and third parties are obligated 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.

6.0 ICT Projects Management

- OPEnE shall ensure that ICT conforms to the if there are any ICT projects management procedures and complies with all internally developed procedures for managing projects.
- OPEnE management team will monitor the key Challenges if any ICT projects are undertaken and provide regular progress reports on identified risks and preventive/detective actions taken.

6.1 Procurement of ICT Equipment and Services

- OPEnE management will implement the necessary controls to ensure that all ICT procurements are done in line with the requirements of the organization
- User or Departments shall establish and submit, in writing, all ICT-related requirements whether ad-hoc or planned, to ICT focal point, who will process and submit them to the procurement unit after the relevant authorization.

- ICT Focal point, shall ensure that all requirements for ICT procurements comply with Organisation Standards and Guidelines.
- The procurement unit shall not procure any ICT System, Service, Equipment, Consumables or Accessory if the request is not originating from ICT focal Point and the relevant Management team.

7.0 Applications software and Hardware

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

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

- To ensure the system acquired follows proper procedures;
- To establish controls for the efficient acquisition and administration of applications, and
- To enhance accountability on the management and usage of ICT Applications.

7.1 ICT Hardware and Applications Acquisition/Purchasing and Maintenance

- There shall be clear understandable business and system requirements before any application acquisition.
- User departments shall submit to the management their ICT requirements to be included in the ICT resource budget.
- All applications supplied shall be checked by ICT Focal point to verify whether the technical requirements established are met and approved.
- The ICT Focal Point shall establish appropriate software standards to facilitate acquisition/development.
- The ICT Focal point shall ensure the best configuration is adopted for the system acquired.
- Only the Admin Coordinator is allowed to purchase IT-related equipment under the supervision of the Team Leader.
- The general procurement procedure should be followed for purchasing
- All IT equipment values more than Rs.10,000/= must be included in the asset list including the value and the date of purchase
- Admin Coordinator must maintain a separate user list for laptops, flash drives and external hard disks. The capacity, model, and IMEI numbers should be included and the updated list should be sent to Team Leader every quarter
- Only the IT focal points are allowed to install software on OPEnE's computers. Under normal circumstances in no case are users allowed to install privately

bought/obtained software or downloaded software on OPEne's computers/notebooks.

- Software and hardware on each computer shall be audited regularly (compliance check). OPEne has the right to delete all illegal or not approved programs from IT equipment owned by OPEne. The IT focal point is responsible to check each computer at least once a year. This is to be documented properly.
- In case of problems with the IT equipment, the user contacts the IT focal point for initial troubleshooting. If the problem cannot be solved internally, the IT focal point may request external IT support.

7.2 Applications Maintenance and Support

- Administration and maintenance of applications shall be an ongoing process that will last throughout the life cycle of the application.
- Every application acquired by the organization shall have documentation in place and updated regularly.
- Installation of additional applications or overriding existing ones shall follow change management procedures.
- Software acquired for installation into the organization's equipment shall be licensed as much as possible.

8.0 ICT Infrastructure

ICT infrastructure supports OPEne's 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, laptops, storage, back-up, operating facilities**, and supporting platforms like operating systems and databases.

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

8.1 Infrastructure Planning and Design

- OPEne shall ensure that ICT infrastructure architecture is in place and in line with the organization's current and future requirements.
- OPEne shall ensure that appropriate ICT infrastructure is set up for the Organisation and well managed by the ICT Focal Point.

8.2 Data Management and Storage

- OPEnE's business-related data shall be stored in a way to facilitate backup procedures and access.

8.3 ICT Equipment and Hosting

- OPEnE shall acquire desktop computers, laptops, OPEnE printers, and networking equipment from authorized suppliers.
- All ICT resources shall be acquired in consultation with the relevant management team
- OPEnE shall establish an appropriate environment for hosting computing and storage equipment based on standards and best practices.

8.4 Infrastructure Maintenance and Support

- OPEnE shall ensure that all ICT infrastructure components are maintained at a reasonable operational and secure level.
- OPEnE shall ensure that a standard software list including the operating system to be installed into the organization's equipment is established.
- OPEnE shall ensure that maintenance services are procured in consultation with ICT focal point as necessary.

9.0 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.

9.1 The objectives of ICT Service Management are:

- To improve internal and external stakeholders' satisfaction.
- To assist in defining meaningful metrics to measure service results and using the metrics to drive continuous service improvement.
- To enable the monitoring and improvement of service quality through the effective application of processes.
- To ensure compliance with all eGovernment Standards and Guidelines relating to the ICT Service Management

9.2 ICT Service Desk

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

9.3 Management of Service Levels

- OPEnE shall ensure that for every ICT service provided, a clear record will be maintained.
- OPEnE shall ensure that reports on service quality are reviewed periodically with users in order to determine things that could be added or changed to improve service delivery and support.

9.4 Management of Third-Party Services

- OPEnE shall ensure proper processes and procedures for managing vendors are in place.
- OPEnE shall ensure that services procured from third parties (suppliers, vendors and partners) meet business requirements.
- OPEnE shall ensure that it builds good relationships with the business and third-party providers to ensure that ICT services delivered continue to meet evolving organization's business needs.

9.5 ICT Service Requests, Incidents, and Problems Management

- OPEnE 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.
- OPEnE shall ensure that Service Requests and Incidents Management processes and procedures are established to ensure minimal adverse impacts on customers.
- OPEnE management shall review all reports about problems that resulted in systems downtime to identify the root causes of problems.

9.6 Change Management

- OPEnE shall ensure that a process for recording, assessing, and authorizing all changes prior to implementation, including changes in procedures, processes, systems, and service parameters is established.

9.7 ICT Service Availability

- OPEnE shall implement an availability management process to ensure that services are available when needed

9.8 ICT Service Continuity

- OPEnE shall conduct an analysis to identify critical functions to be supported by ICT focal point and Admin.

- OPEnE's shall ensure that service continuity and recovery plans are in place and that these plans are regularly reviewed and tested and that key staff is appropriately trained.
- All information regarding ICT assets, Service Level Agreements, End User documentation version control, and change requests shall be kept up to date and secure place

9.9 Capacity Management

- OPEnE shall establish a capacity plan to monitor ICT resource usage for existing and planned systems in order to assist in the time and cost-effective purchase of additional resources so as to avoid panic purchases when resources run out.

9.10 Data Management

- OPEnE's program requirements for data management shall be determined and unauthorized/illegal data not be stored in OPEnE's ICT equipment or cloud storage
- OPEnE shall develop procedures for effective and efficient data storage, retention, and archiving to meet organizational objectives, the organization's ICT Policy, and regulatory requirements.

10.0 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 OPEnE with information security mechanisms to support the organization to achieve its strategic goals based on best practices.
- Protection of the OPEnE's ICT resources from accidental or malicious activity while preserving the open information sharing requirements of the Government, and Making the OPEnE's stakeholders aware of their responsibilities with respect to ICT security.

10.1 ICT Security Management

- OPEnE shall actively support ICT security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of ICT security responsibilities.
- OPEnE 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.
- ICT Policy shall be established to highlight the implemented ICT security controls that ensure 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.

- All users of OPEnE's systems shall be responsible for protecting the organization's information resources.
- OPEnE shall retain overall responsibility and ownership for all organization's information assets.
- An up-to-date Anti-Virus tool, as well as a personal firewall guard, has been installed to protect each computer of OPEnE. The user is not allowed to shut down either of them. Users may contact the IT focal point immediately if they think the Anti-Virus tool and/or Firewall is not functioning properly.
- Special caution needs to be maintained when using portable devices (such as memory sticks, memory cards from digital cameras, CD-ROMs, DVDs, external hard drives, etc.). Some of which may be infected with viruses, worms, or Trojans and therefore pose a considerable threat to computers and network security. It is obligatory to virus-check these devices before accessing the data.
- Users are not to conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the OPEnE network or the internet or bypass security features.
- Users are not allowed to download any software from the internet nor to install the software (including updates and patches) without prior approval. Only the IT focal point is authorized to install pre-approved software.

10.2 Laptop/mobile devices

- Portable equipment is always open to the risk of being stolen. You must not leave equipment (laptop, memory sticks, and external hard drives) unattended. Equipment shall always be locked overnight and not left on desks.
- If you carry a laptop or other equipment, keep it with you when traveling. Wherever practical, do not leave it in empty cars, hotel rooms, etc. Do bear in mind that it is not just the equipment that can be stolen – the data on the drives will go as well.
- Any data, which has to be stored on a laptop, shall be regularly backed up. It is the responsibility of the user that this is done. The IT focal point can assist and also provides an external hard drive or server access for the backup.
- Users are responsible for the Mobile assets which are allocated under their name and if there is any physical damage caused by careless or improper usage then they will have to bear the cost.

10.3 Monitoring

- OPEnE will monitor the 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, text messages, the telephone system, voicemail and mobile telephone logs, access control logs, and CCTV recordings. This is to ensure that the organization's business interests are protected, for quality control purposes, to detect abuse of the systems, or to detect or prevent crime or misconduct.

11.0 User policy (User ID, Password, Internet, and email)

11.1 User ID and Password

- Every user logs on (limited access only) to the assigned computers with a unique username (ID) and password.
- User ID will be allocated based on their name with Initials.

11.2 Password policy

- Standardize Password Length and Combinations.
- mix with letters, numbers, and Special characters
- Limit Password Attempts and Implement a Lock-Out Policy.
- Change Passwords Every 180 Days.
- Use Multi-Factor Authentication.
- not to share with anyone else
- system will be locked or log off by pressing CTRL + ALT + DEL

11.3 Internet Policy

- Access is provided for use in connection with OPEnE's work – it is not intended for private use, but occasional use is permissible, as long as the user adheres to this policy and services for others are neither disrupted nor unnecessary/additional costs for OPEnE incur.
- Under no circumstances must software be downloaded (programs, Movies, games, etc.).
- The user shall not participate in online Movies, games or any other illegal activities using the IT resources of OPEnE.
- The internet must not be used for downloading large images, videos, music, etc., or accessing newsgroups and chat rooms which is not for OPEnE use.
- Deliberate and unauthorized accessing or downloading of pornographic, offensive, illegal, obscene, or indecent material at any time is forbidden.
- OPEnE may monitor or has the authority to monitor and record details of all internet uses and attempted access to restricted sites. Although OPEnE may monitor and

block access to sites, it cannot necessarily protect users from material that they may find offensive.

- If access is required to a blocked site, or a user believes a site should be blocked, contact the IT focal point.
- To protect the privacy of the user, the “remember password “-function shall not be enabled.
- OPEnE reserves the right to block access to any sites it finds necessary

11.4 Email policy

General

- Eligible employees who require email for work purposes and are basic computer literate as well as possess a basic command of English may request OPEnE an email address. After approval by the Team Leader, the IT focal point or the Admin & Coordinator may issue an email address. The IT focal point records all created OPEnE-email addresses in a list.
- For each OPEnE's email address in Gmail will be set up/configured. The IT-focal point is responsible for this.
- Email Access is provided for use in connection with work related to OPEnE – it is not intended for private use, but occasional use is permissible, as long as the user adheres to this policy and provided large attachments are not transmitted.
- The use of personal email accounts for OPEnE business is not usually allowed. But will be considered if there is a valid reason.
- Any Email must not contain anything that could be considered defamatory, discriminative, pornographic, offensive, obscene, or indecent. Misuse will be investigated and if substantiated may lead to disciplinary measures.
- Opening Email attachments are the most common route for a computer virus to infect a computer and network. Attachments **MUST NOT** be opened if they come from an unknown source or if there is any doubt regarding the originator. If in doubt, the user may contact the IT focal point immediately.
- If a user has no access to his Emails (e.g. during leave), an automatic Out-of-office-reply can be created, using the Auto-Response-Function under Options in OPEnE-Gmail, to inform the sender about the absence of the recipient.
- Email user identities and personal passwords must not be shared with others and staff should be wary of providing their email addresses to external parties, especially mailing lists.

11.5 Webmail

In addition to accessing, one's email on one computer, OPEnE email may be used to address one's emails from any computer in the world with internet access. When using OPEnE email in public internet cafes, particular care needs to be exercised in ensuring that your login and password are kept secret and not stored on the computer. You should exit the browser before logging off. Under no circumstances whatsoever must the 'remember password' option be used to access OPEnE's email.

11.6 Email Tips

- Take the same care when writing Emails as you would for a written document
- Always remember that nothing written in an Email is confidential. Therefore, do not communicate sensitive data, confidential personal information, passwords, etc. via email.
- Read your mail a minimum of twice a day.
- If possible, reply within 24 hours to an Email that is directly addressed to you and requires your answer.
- Make the "subject" field of your message as meaningful as possible – this will help your recipient.
- Keep your Inbox tidy. Move Emails to sub-folders or delete them, if no response is needed.
- Do not print emails unless necessary.
- Use a signature that gives your name, position within OPEnE, phone number, email, web address, and Facebook page of OPEnE.
- The best way to deal with 'junk' email is to delete it.

12.0 Approved Software

- To ensure common software standards within the organization and to enable efficient maintenance and trouble-shooting only pre-approved software may be installed on OPEnE's IT equipment by the IT-focal point.
- The current list of OPEnE-approved and not-approved software is found in Annex 1. No other software is to be installed. The list of approved software will be revised as needed and updated periodically. Exemptions may be made if users require special software for work at OPEnE (e.g. publishing, designing software). The IT focal point should be kept informed to enable them to document this in the IT-inventory list.
- It is encouraged original software is to be installed on OPEnE computers and the IT-focal point ensures that sufficient licenses are available for standard software such as MS Office.

12.1 Minimum configuration standard

- To enable efficient maintenance and trouble-shooting all OPEnE, computers are identically configured according to the OPEnE configuration standard
- Any deliberate non-compliance with this policy, particularly where this involves offensive behavior or a potential breach of computer security, will be dealt with by Team Leader, direct supervisor and in consultation with the IT focal point. The disciplinary procedures as laid out in the ToE shall be followed.
- It is the responsibility of each employee and every individual attached to OPEnE to adhere strictly to all aspects of this policy. If you need further clarification and assistance, please contact the security focal points.

13.0 Using the network and Printers

- Each user is responsible to ensure monthly backup of all user data on external or network drives or Cloud storage such as Google Drive or One drive or any other cloud services which are approved by the OPEnE
- Users must not attempt to gain access to systems or information for which they are not authorized.
- If users believe to have access to unauthorized systems, software, or data this should be immediately reported to the IT-focal point and the Program Manager.
- Printing and photocopying facilities are strictly for official purposes and should not be misused

14.0 Implementation, Reviews and Implementation

Implementation and Reviews

- This document shall come into operation once tabled and agreed upon in the Board meeting, and approved on its first page, and then shall be considered mandatory for all OPEnE program operations.
- All employees and other authorized users of OPEnE shall comply with the requirements of this policy.
- The Admin Coordinator responsible for ICT(reporting Line of ICT focal point) shall enforce compliance by using audit trails and triggering access denial to OPEnE systems and networks.
- OPEnE staff found to have violated this policy may be subject to withdrawal and or suspension of systems and network privileges or disciplinary action in accordance with rules defined by OPEnE administrative regulations.
- This document shall be reviewed as needed whenever the business environment of OPEnE changes in a way that affects the current policy.

14.1 Exceptions

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

15.0 Roles and Responsibilities

ICT Steering Committee

- Shall propose OPEnE's ICT Policy for the consideration of the board;
- Shall coordinate the establishment and continues review of OPEnE 's ICT Policy, ICT Strategy, and Enterprise Architecture
- Shall ensure that the ICT Strategy/Implementation is aligned with OPEnE's Organisation Plan;
- Shall advice the board in making considered decisions about the focus of ICT resources;
- Shall review all ICT services and applications including OPEnE's website and infrastructure with the view to advice OPEnE on required improvements; and
- Shall ensure that risks associated with ICT are managed appropriately

Team Leader/ Coordinators/ICT Focal Point.

- Shall ensure that all users under their supervision are aware of and comply with this policy;
- Shall provide adequate and appropriate protection of ICT assets and resources under their control;
- Shall ensure availability, integrity, and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations; and
- Shall review and approve procedures, standards, policies, and guidelines developed from this policy for the purpose of maintaining business continuity and security of OPEnE 's ICT resources.
- Shall be the custodian of "Data and Information" for their respective Departments/sections/Units.

ICT- Focal point

In order to ensure standardized and high-quality IT support as well as to properly guard the implementation of this policy, every OPEnE's office must have one staff member appointed as the IT focal point. This person is responsible for

- Monitoring the implementation of this policy

- The installation of new hardware and devices.
- The installation of the pre-approved standard software on all computers (Annex 1).
- To maintain OPEne's IT inventory list (Annex 2).
- To create user accounts (password-protected and limited access) on individual computers for eligible employees.
- Only the IT-focal points and one PMT member will have Administrator-privileges on computers.

Internal Audit Unit

- Shall audit the ICT Function of OPEne and ensure compliance with the policy.

Users of ICT Systems

- Shall be responsible to safeguard ICT assets of OPEne in their custody.
- Shall comply with this policy.

Monitoring and Evaluation

- ICT Steering Committee shall meet at least quarterly to monitor and evaluate the achievements in ICT initiatives against OPEne ICT Policy, Strategic Plan, and Architecture of the Organization's ICT.

Annex 1 – Approved Software

Software	Versions
Operating System	Microsoft Windows(10/11) /iOS/Android
Application software:	Microsoft Office Google Suite Adobe Acrobat Reader Version 7 ZIP -File Extractor Zoom /google meet/ Microsoft Teams Typing Master Windows Media Player/VLC Media player Video downloader WhatsApp Photoshop /Canva/AutoCAD as needed
Antivirus Software	Windows defender Kaspersky Internet Security

