1 of 2

Security Classification: Restricted

SEP-IMT-GEN-IT02-00043

ELECTRONIC INFORMATION & COMMUNICATION SYSTEM

EXECUTIVE SUMMARY

October 2025

Rev	Date	Description	Issued by	Checked by	Approved by
A03	27-10-2025	Issued for Approval	D. Osemwegie	R. Brown	U.U. Udoma

ADDITIONAL APPROVAL / REVISION HISTORY TABLE

Party	Name	Sign	Date

Revision Philosophy

- All documents for review will be issued at R01 as required, with subsequent R02….
- If the document is for information, it will also be issued as A01.
- All revisions Issued for Approval/Implementation will be issued at A01, with subsequent A02, A03, etc. as required.
- All revisions approved for design will be issued at D01, with subsequent D02, D03, etc. as required.
- Documents approved for Construction will be issued at C01, C02, and C03 respectively.
- Documents or drawings revised as “As built” will be issued as Z01, Z02 Z03 etc.
- Narrative sections revised from previous approved issues are to be noted in the table below and/or highlighted in the RH margin (using the appropriate revision status) thus: | A02.
- Previous revision highlighting to be removed at subsequent issues.
- Drawings/diagrams revised from previous approved issues are highlighted by 'clouding' the affected areas and by the use of a triangle containing the revision status.

Revision History

Revision No.	Date of issue	Reason for change
1.0	29th of January 2016	To amend policy account holder
2.0	27th October 2020	Revised Update
3.0	27th October 2025	Revised Update

1.0 INTRODUCTION

Seplat Energy Plc. ("Seplat" or the "Company") makes a significant investment in communications systems and equipment. Seplat's communications systems and equipment are used by its workforce, consultants, or agents of Seplat or its suppliers who are given access to Seplat's communications systems and equipment from time to time. Seplat's electronic communications systems and equipment are intended to promote effective communication and working practices within the Company and are critical to its success.

This Electronic Information and Communication Systems Policy (the "Policy") has been established to protect the Company's investment in its electronic communications equipment, protect and control all Seplat's systems, safeguard the client data and information within these systems, reduce business and legal risks and protect the good name of the Company as well as enhance the Company's general performance.

Seplat Workforce and other persons given lawful access to the company's electronic communications systems and equipment are expected to always protect the Company's electronic communications systems and equipment from unauthorized access and harm. Failure to do so will attract the Seplat Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

a. Policy Statement

This Policy deals mainly with the use (and misuse) of computer equipment, email, the internet, telephones, smart phones, personal digital assistants ("PDAs") and voicemail. It applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards.

This Policy outlines the standard compliance required from users of Seplat's systems the circumstances in which the Company will monitor use of these systems as well as consequences of violations.

b. Objectives

The purpose of this document is to:

- To enhance operational efficiency and decision-making through the real-time exchange and management of information across all levels of Seplat Energy Plc.
- To ensure robust security protocols are in place to protect sensitive data and mitigate the risk of cyber threats and unauthorized access.
- To comply with industry standards and regulatory requirements for electronic communication, ensuring the integrity and confidentiality of information.
- To provide a scalable and flexible platform that supports the evolving technological needs of the company, facilitating innovation and digital transformation.

- To implement comprehensive risk management and control measures that monitor system performance, manage data retention, and ensure business continuity.

c. Applicability and Scope

This Policy shall apply to Seplat Directors, Seplat Workforce, consultants or agents of Seplat or its suppliers who are given access to Seplat's communications systems and equipment from time to time. This Policy also applies to Seplat's information technology service providers and contractors.

2.0 RELATED DOCUMENTS

This document serves as an Executive Summary of the Electronic Information & Communications System Policy. For more comprehensive details and guidelines for implementation, the full policy should be read. Other policies include the Company's Communication Policy, Acceptable Use Policy, Generative AI Acceptable Use Policy, and the Code of Business Conduct.

POLICY OWNER: CHIEF EXECUTIVE OFFICER

2 of 2

Seplat energy

Security Classification: Restricted

SEP-IMT-GEN-IT02-00043

ELECTRONIC INFORMATION & COMMUNICATION SYSTEM

MAIN CONTENT

October 2025

TABLE OF CONTENTS

1. DEFINITIONS

Terms	Definition
Electronic Information	Electronic Information refers to any data received, communicated, or stored digitally.
Person(s)	Refers to one or more members of the SEPLAT Workforce
Workforce	All employees, contract staff, contractor staff, consultants or any other person engaged in the operations of SEPLAT. This Policy refers to these individuals as **"Workforce"** for simplicity of reference only, and no further meaning shall be implied and construed by such reference.

Abbreviation	Meaning
CCTV	Closed-Circuit Television
CD	Compact Disc
CS	Company Secretary
IT	Information Technology
MMS	Multi-Media Messaging Service
PC	Personal Computer
PDA	Personal Digital Assistant
SMS	Short Message Service
USB	Universal Serial Bus

2. ROLES AND RESPONSIBILITIES

2.1. The Head of IT Department shall:

a. Manage access controls for all computer systems, maintain and secure the list of administrative access codes and passwords, and ensure that members of the technical unit understand the importance of preventing unauthorized access.
b. Install and maintain updated anti-virus software on all computers, respond urgently to virus threats, keep the anti-virus server current, and ensure that members of the Workforce do not have administrative rights on the network.
c. Ensure that all work data is stored on network drives and that no member of the Workforce stores critical data on local PC/Laptop drives. Develop, implement, and maintain a security awareness and training plan.
d. Maintain a record of software licenses owned by the company and periodically scan computers to confirm that only authorized software is installed.
e. Responsible for all equipment installations, disconnections, and modifications.

2.2. All Workforce shall:

a. Be responsible for the security of allocated equipment and ensure that it is not used by unauthorized individuals. Keep passwords confidential and change them regularly.
b. Treat all information accessible on group systems confidentially and not access any information they are not entitled to unless specifically authorized.
c. Not download or install software from external sources without authorization from the IT Department.
d. Use email and internet services responsibly, ensuring that all communications are professional, and that confidential information is not sent without encryption
e. Exercise caution when opening emails from unknown sources and inform the IT Department immediately if a suspected virus is received.
f. Adhere to the Company's policies on the use of systems and understand that misuse or excessive use may be treated as a disciplinary matter.

3. ADMINISTRATION OF POLICY

3.1. Seplat's management is responsible for the administration of this policy. Each member of the Workforce and any person that signs this policy acknowledge receipt of same.
3.2. This policy will be updated periodically, and each update will become effective from the date appropriate Persons are made aware of it by Seplat's management.
3.3. Seplat's managers and supervisors are to ensure that all appropriate members of the Workforce are aware of this policy (and any update thereof) and the location of this policy is known.

4. EQUIPMENT SECURITY AND PASSWORDS

4.1. The Head of Information Technology Department (the "IT Department") shall ensure that his/her department undertakes administration of access controls of all computer system, maintains, and secures the list of administrative access codes and passwords and ensure that members of the technical unit are apprised of the seriousness of any unauthorized access.

4.2. All Persons given access to Seplat's electronic communications and equipment shall:

a. Be responsible for the security of the equipment allocated to or used by him/her.
b. Must not allow it to be used by anyone other than as permitted by the IT Department.
c. Be responsible for the security of his/her terminal. In leaving a terminal unattended or on leaving the office, each Person should ensure that they lock their terminal or log off to prevent unauthorized users accessing the system in his/her absence.
d. Not tamper with Desktops PCs and cabling for telephones or computer without first consulting the IT department.
e. Keep passwords confidential and must not make them available to anyone else unless authorized by the IT department. Passwords are unique to each user and must be changed regularly to ensure confidentiality. For the avoidance of doubt, on the expiry or termination of employment (for any reason), member of the Workforce must provide details of his/her password to the HR department and return any equipment, key fobs or cards allocated to such Person.
f. Endeavor to use passwords that will not be easily guessed by others or record same where they may not be easily obtained. Passwords must be changed immediately if it is suspected that they may have become known to others.
g. Ensure that all information accessible on group systems are treated confidentially and not access any such information which they may not be entitled to in the course of their duties unless specifically authorized.
h. Ensure that client data and information may not be printed, copied, removed, amended, deleted without approval from the CS before approving selection.
i. Obtain approval from their respective divisional head before any company data can be removed from any PC, laptop or network share. No copies of CDs or DVDs or any media are allowed without the authorization from the IT department.
j. Not attempt to gain access to restricted areas of network, or to any password protected information, unless specifically authorized.

k. Where issued with a laptop, PDA, or smart phone, ensure that it is always kept secure, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft.
l. Exercise reasonable caution when using equipment away from the workplace because documents may be read by third parties, for example, passengers on public transport.

5. SYSTEMS AND DATA SECURITY

5.1. Members of the Seplat Workforce are not allowed to delete, destroy, or modify existing systems, programs, information, or data which could have the effect of harnessing the Company's business or exposing it to risk.
5.2. Viruses can cause destruction of corporate resources and are easier prevented than cured. Seplat monitors all emails passing through its system for viruses.
5.3. The Head of the IT Department shall be responsible for ensuring that the department:
a. Installs and maintains appropriate and updated anti-virus software on all computers.
b. Responds urgently to all virus threats and detect and destroy any virus and keep appropriate documentation for each incident.
c. Ensures that the anti-virus server is up to date.
d. Ensures that other members of the Workforce do not have administrative rights on the network.
e. Ensures that all work data is stored on the network drives and that no Person has critical data on the local PC/Laptop
f. Develops, implements, and maintains a security awareness and training plan. This plan shall include the schedule for staff security training, education, and awareness and ensure that all Persons understand their role in protecting the confidentiality and integrity of data.
5.4. Members of the Seplat Workforce shall:
a. Not knowingly introduce a computer virus into the company computers
b. Not download or install software from external sources without authorization from the IT Department. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the IT Department before they are downloaded. The following shall not be accessed from the network online radio, audio and video streaming, instant messaging and webmail (such as Whatsapp, Snapchat, Gmail, Hotmail, or Yahoo) and social networking sites (such as Facebook, YouTube, X (twitter, Instagram). The company reserves the right to modify this list from time to time.

c. Not attach any device or equipment to the company systems without the prior approval of the IT Department. This includes any USB flash drive, MP3 or similar devices, PDA, Bluetooth Adapters or smartphones. It also includes use of USB port, infra-red or connection port or any other port.
d. Exercise caution when opening emails from unknown external sources or where, for any reason, and email appears suspicious. The IT Department should be informed immediately if a suspected virus is received. The company reserves the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this policy. The company also reserves the right not to transmit any email message.
e. Be particularly vigilant when using Seplat laptops or Wi-Fi enabled equipment outside the office and shall take any precautions required by the IT Department from time to time against importing viruses or compromising the security of the company's system or information which is confidential to the company's business.
f. Not uninstall, stop or change the configuration of any anti-virus software. Incoming diskettes/drives/removable drives/cd's should be scanned for viruses before they are read.

5.5. Any Person who suspects that his/her system has been infected by a virus shall immediately contact the IT Department for immediate assistance.

6. PHYSICAL SECURITY

6.1. It is the company's policy to protect its computer hardware, software, data and documents from misuse, theft, unauthorized access, and environmental hazards.

6.2. Members of the Workforce should ensure that:
a. Diskettes/CDs are stored out of sight when not in use and locked up where they contain highly sensitive information.
b. Diskettes/CDs are kept away from environmental hazards such as heat, direct sunlight and magnetic fields.
c. The IT department is responsible for all equipment installations, disconnections and modifications. Other members of the Workforce should not undertake those activities.
d. Exercise care to safeguard all valuable electronic equipment assigned to them and
e. Environmental hazards to hardware such as smoke, liquids, extreme heat, etc are always avoided.

7. COPYRIGHTS AND LICENSES

7.1. It is the company's policy to comply with all laws regarding intellectual property. All source code, business solutions, applications that are developed, designed or created for the company belongs solely to it.

7.2. The Head of the IT Department should ensure that the IT Department maintains record of software licenses owned by the company and that computers are scanned periodically to confirm that only authorized software is installed.

7.3. No Person shall install, copy or download software unless authorized by the IT Department.

8. EMAIL ETIQUETTES AND CONTENT

8.1. It is the policy of the company to provide email to all members of the Workforce, whenever possible when required by their job functions. Each Person should note that correspondences via emails are not guaranteed privacy and must ensure that confidential emails are not sent without encryption.

8.2. Email is a vital business tool and means of communication and should be used with great care and discipline. Members of the Workforce should always consider if email is the appropriate means for a particular communication and whether the tone of the email is appropriately formal for the subject matter of the communication. Correspondence sent by email should be written as professionally as a letter or fax. Messages should be concise and directed only to relevant individuals. The company's standard disclaimer should always be included at the foot of every email.

8.3. No Person shall send abusive, obscene, discriminatory, racist, harassing, derogatory, or defamatory emails. An Person who feels that he/she has been harassed or bullied or offended by material received from the colleague via email should inform his/her line manager of the human resources department.

8.4. Members of the Workforce should take care with the content of email messages as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Every Person should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

8.5. Email messages may be disclosed in legal proceedings in the same way as paper documents. Detection from your inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

8.6. In general, members of the Workforce should not:

a. Send or forward private emails at work which they would not want a third party to read.

b. Send or forward chain mail, junk mail, cartoons, jokes, or gossip.

c. Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them.

d. Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship, or charitable appeals.
e. Agree to terms, waive the rights of the company, enter contractual commitments, or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter.
f. Download or email text, music, and other content on the internet subject to copyright protection, unless the owner of such works allows this.
g. Send messages from another worker's computer or under an assumed name unless specifically authorized or
h. Send confidential messages via email or the internet, or by other means of external communication which are not secured.

8.7. Any member of the Workforce who receives a wrongly delivered email, should return it to the sender. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

9. USE OF THE INTERNET

9.1. The provision internet /intranet privileges and access to computer systems and networks by the company are intended for business purposes only. Use of same is subject to monitoring for security and/or network management.

9.2. When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 11.2, it could be a source of embarrassment to the company, especially where inappropriate material has been accessed, downloaded, stored, or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence where for instance the material is pornographic in nature.

9.3. Members of the Workforce are prohibited from accessing any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. Even where such content may be legal in Nigeria or in any other jurisdiction, it is still prohibited so far as such content is immoral and/or presents the company in a bad light. As a rule, if any person might be offended by the contents of a page, or the fact that our software has been accessed the page or file might be a source of embarrassment if made public, then viewing it during working hours or at any time whilst on company property or using company equipment, will be a breach of our Electronic Information and Communications Systems Policy.

9.4. Use the company's systems by any Person, to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or micro-blogging platforms is strictly prohibited.

10. PERSONAL USE OF SYSTEMS

10.1. The company permits the incidental use of internet, email, and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and the company reserves the right to withdraw the privilege of personal use of systems at any time.

10.2. The following conditions must be met for personal usage to continue:

a. Use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 8am or after 5pm)
b. Personal emails must be labelled “personal” in the subject header.
c. Use must not interfere with business or office commitments.
d. Use must not commit the company to any marginal costs, use must comply with Seplat’s code of Business Conduct and any other policies or procedures which may be included in the staff handbook or adopted by Seplat from time to time.
e. Such personal emails must not breach this policy in any way.

10.3. Personal use of the company systems may be monitored and, where breaches are found, disciplinary action may be taken. Seplat reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive.

11. MONITORING OF USE OF SYSTEMS

11.1. The systems enable the company to monitor telephone, email, voicemail, internet, and any other communications. For business reasons, and in order to carry out legal obligations of the company, use of the systems including the telephone and computer systems and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary as justifiable for ensuring compliance with this policy and for any business purposes.

11.2. A CCTV system monitors the exterior of the company’s property and sites 24 hours a day. This data is recorded.

11.3. The company reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

a. To monitor whether the use of the email system or the internet is legitimate.
b. To find lost messages or to retrieve messages lost due to computer failure.
c. To assist in the investigation of wrongful acts or
d. To comply with any legal obligation

12. INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

12.1. Access is granted to the internet, telephones, and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it

is in full compliance with our rules, policies, and procedures (including this policy, Seplat's Code of Business Conduct and any other policies or procedures which may be included in the Staff Handbook or adopted by Seplat from time to time.

12.2. Misuse or excessive use or abuse of our telephone or email system, or inappropriate use of the internet in breach of this policy will be dealt with as a disciplinary matter. Misuse of the email system or inappropriate use of internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting, or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

a. Pornographic material (that is, writings, pictures, films and video clips of a sexually explicit or arousing nature)
b. Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients.
c. A false and defamatory statement about any person or organization
d. Material, which is discriminatory, offensive, derogatory or may cause embarrassment to others.
e. Confidential information about Seplat or any member of its Workforce or clients
f. Any other statements which is likely to create any liability (whether criminal or civil, and whether for the individual or Seplat.
g. Material in breach of copyright

12.3. Any such action will be treated very seriously and is likely to result in summary dismissal.

12.4. Where evidence of misuse is found, the company may undertake a more detailed investigation involving the examination and disclosure of monitoring records to these nominated to undertake the investigation and any witnesses or managers involved. If necessary, such information may be handed to the police in connection with a criminal investigation.

13. USE OF SOCIAL MEDIA

13.1. "Social Media" means, but is not limited to, applications such as Facebook, X (Twitter), Instagram, Pinterest, Quora, etc.

13.2. Use any form of social media, on work or personal desktop computers, laptops, mobile phones or smart phones, during their working hours is strictly prohibited, except for legitimate business purposes.

13.3. Members of the Workforce shall not interact or contact clients, visitors, or any other non-company persons via social media or any other form of communication - including SMS (Short Message Service) or MMS (Multimedia Messaging Service), unless for legitimate business purposes or if such persons are personal friends, family, or acquaintances.

13.4. Use of business mediums, such as LinkedIn, will be permitted where it is appropriate to develop business clients/relations.

13.5. Seplat expects members of the Workforce to use social media (during their personal time) responsibly and safely and adhere to the following guidelines:

a. Posting disparaging or defamatory statements about Seplat, its clients and other affiliates and stakeholders is strictly forbidden.
b. No Person shall do anything to jeopardize Seplat's confidential information and intellectual property using social media.
c. Every Person should respect their colleagues, clients, customers, and stakeholders and should not post anything against those colleagues, customers, clients and stakeholders would find offensive, including discriminatory comments, insults or obscenity.

14. CONSEQUENCES OF VIOLATIONS

14.1. Any Person found to have violated or be in breach of this Policy may be subject to disciplinary action, where such person is a member of the Workforce, such action will be in accordance with the Company's disciplinary procedure, as referred to in Seplat's Staff Handbook.

15. CONFIDENTIALITY UNDERTAKING

15.1. "Confidential Information" is any information relating to the business, affairs, customers, clients' suppliers, plans, intentions, market opportunities, trade secrets, secret formulas, processes, business and marketing plans, salary structure, contracts or details of computer systems of the Company which is proprietary to the Company or would normally be regarded as confidential by a reasonable person.

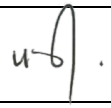
15.2. To protect the goodwill and interests of the Company and its Confidential Information, each member of the Workforce is required to maintain the confidentiality of all such Confidential Information and to give the Company the undertaking set out in this document.

15.3. Members of the Workforce shall not directly or indirectly divulge or disclose any Confidential Information to any other persons, company, or concern without the prior written consent of the Company.

16. EXCEPTION AND AMMENDEMENT

16.1. This policy will be reviewed by the Board annually and at such other times as circumstances may require. This policy may only be amended, or its requirements varied, in relation to individual circumstances, with the approval of the Board.

16.2. This policy has been approved by the following authorized individuals:

Name	Title	Signature	Date
Roger Brown	Chief Executive Officer		
Udoma Udo Udoma	Board Chairman		

Contact Information
For any questions or clarifications regarding this policy, please contact:

- **Department:** IT Department
- **Email**: ITDept@seplatenergy.com