AKWA IBOM STATE HOUSE OF ASSEMBLY

A

BILL

FOR A LAW TO PROVIDE FOR THE GOVERNANCE, RESPONSIBLE DEVELOPMENT, REGULATION AND ETHICAL ADOPTION OF ARTIFICIAL INTELLIGENCE IN AKWA IBOM STATE AND FOR RELATED MATTERS

Sponsor: Hon. (Engr.) Uduak-Obong Ekpo-Ufot

Co-Sponsors:

Rt. Hon. Kufreabasi Edidem

Rt. Hon. (Barr.) Otobong Bob

Hon. (Dr.) Nsidibe Akata

Hon. Sunday Udofot Johnny

Hon. (Engr.) Udobia Udo

Hon. (Engr.) Ubong Attah

Hon. (Dr.) Itoro Etim

Hon. Jerry Otu

Hon. Prince Aniefiok Attah

Hon. Bassey Pius Bassey

Arrangement of sections

PART I

Objectives and Scope of Application

1. Objectives

2. Scope and application

3. Relationship with Federal laws and regulators

4. Guiding principles

PART II

Akwa Ibom State Artificial Intelligence Council

5. Establishment of the Council

6. Functions of the Council

7. Composition

8. Appointment, qualifications and tenure

9. Independence and conflicts of interest

10. Cessation and removal

11. Meetings and quorum

12. Director-General

13. Technical Evaluation Panel

14. Staff and consultants

15. Training and capacity building

16. Regulations and guidelines

PART III

Risk-Based Governance of Artificial Intelligence

17. Risk classification

18. Prohibited AI systems

19. High-risk AI systems

20. High-risk obligations

21. AI Impact Assessment

22. Registration

23. Limited-risk AI systems

24. Minimal-risk AI systems

25. Reclassification and appeal

PART IV

Rights, Transparency and Responsible AI

26. Transparency

27. Human oversight

28. Right to human review

29. Right to reasons and correction

30. Fairness and non-discrimination

31. Accessibility and inclusion

32. Complaints and redress

33. Trade secrets and security-sensitive information

PART V

Data Governance, Privacy and Cybersecurity

34. Compliance with data-protection law

35. Data governance

36. Data Protection Impact Assessment

37. Cybersecurity

38. Serious AI incident reporting

39. Data localisation and State data sovereignty

PART VI

Artificial Intelligence in Government

40. Responsible government use

41. Government AI Register

42. Government AI Impact Assessment

43. Responsible AI procurement

44. Algorithmic accountability

45. Annual State of AI report

PART VII

Regulatory Sandbox and Innovation

46. Establishment of sandbox

47. Eligibility

48. Safeguards and testing limits

49. Monitoring

50. Exit pathways

51. Effect of State certification

52. Innovation and local content incentives

PART VIII

Compliance, Enforcement and Appeals

53. Supervisory and investigative powers

54. Compliance notice

55. Administrative sanctions

56. Offences

57. Emergency suspension

58. Right to be heard

59. Administrative appeal

60. Judicial review

PART IX

Financial Provisions, Reporting and Accountability

61. Fund of the Council

62. Fees and charges

63. Accounts and audit

64. Annual estimates

65. Annual report and legislative oversight

66. Gifts, grants and procurement

PART X

Miscellaneous

67. Confidentiality

68. Immunity and indemnity

69. Service of notices

70. Judgments and public funds

71. Regulations and standards

72. Review of the Law

73. Transitional provisions

74. Savings

75. Interpretation

76. Short title

Schedules

A LAW TO PROVIDE FOR THE GOVERNANCE, RESPONSIBLE DEVELOPMENT, REGULATION AND ETHICAL ADOPTION OF ARTIFICIAL INTELLIGENCE IN AKWA IBOM STATE AND FOR RELATED MATTERS

BE IT ENACTED by the Akwa Ibom State House of Assembly as follows—

{Commencement: }

PART I

Objectives and Scope of Application

1. Objectives

The objectives of this Law are to

(a) promote safe, responsible, ethical, inclusive development and adoption of artificial intelligence in Akwa Ibom State;

(b) promote the protection of persons from unlawful discrimination, unsafe automated decisions, privacy violations and other significant harms arising from AI subject to applicable Federal Acts and the jurisdiction of competent Federal Authorities;

(c) support research, innovation, entrepreneurship, local content, investment, job creation and digital skills in the State;

(d) establish a proportionate, risk-based framework for AI used, procured, funded or deployed by the State or its public institutions and within matters falling within State competence;

(e) promote responsible AI adoption across State Ministries, Departments and Agencies;

(f) establish a regulatory sandbox for controlled testing of innovative AI systems;

(g) promote transparency, accountability, human oversight and effective remedies within the scope of this Law ;

(h) support the State's development agenda, including economic diversification, youth empowerment and digital infrastructure; and

(i) facilitate cooperation with Federal institutions, regulators, local governments, universities, research institutions, industry and international partners without derogating from the constitutional or statutory powers of competent Federal authorities.

2. Scope and application

This Law applies to the following:

(a) AI systems developed, procured, funded, operated or deployed by Ministries, Departments and Agencies of the State;

(b) AI systems deployed in connection with functions, services, programmes or activities falling within the legislative competence of the State;

(c) AI systems admitted into a State sandbox established under this Law; and

(d) persons or entities that voluntarily participate in a certification, accreditation, testing or sandbox programme established under this Law.

(2) This Law shall not be construed or applied-

(a) to confer on a State or any authority established under this Law jurisdiction over a matter within the exclusive legislative competence of the National Assembly;

(b) to limit, replace or derogate from the powers or functions of a Federal institution, regulator or authority established under the Constitution or an Act of the National Assembly; or

(c) in a manner inconsistent with any applicable Act.

3. Relationship with Federal Laws and Regulators

Nothing in this Law limits or replaces the powers of the National Assembly, a Federal institution or a regulator established the Constitution or an Act of the National Assembly. The Council shall, where appropriate, cooperate with the Nigeria Data Protection Commission and other competent Federal regulators in matters concerning data protection, telecommunications, finance, health, education, critical infrastructure, cybersecurity, competition and consumer protection and other matters within Federal Legislative competence.

4. Guiding principles

Implementation of this Law shall be guided by -

(a) lawfulness and constitutional compliance;

(b) human dignity and fundamental rights;

(c) fairness and non-discrimination;

(d) transparency;

(e) privacy and data protection by design;

(f) safety and cybersecurity;

(g) meaningful human oversight;

(h) inclusion and accessibility;

(i) innovation and technological neutrality; and

(j) social and environmental responsibility.

PART II

Akwa Ibom State Artificial Intelligence Council

5. Establishment of the Council

There is hereby established the Akwa Ibom State Artificial Intelligence Council, a body corporate with perpetual succession and a common seal. The Council shall coordinate the State's AI governance, responsible adoption, innovation and regulatory functions, subject to the Constitution and applicable Act of the National Assembly.

6. Functions of the Council

The Council shall—

(a) develop State AI governance standards and guidelines;

(b) maintain a register of State-government and regulated high-risk AI systems;

(c) conduct or commission risk and impact assessments;

(d) monitor compliance and investigate suspected breaches;

(e) administer the regulatory sandbox;

(f) issue lawful guidance, compliance notices and certificates;

(h) promote research, skills, local content, entrepreneurship and responsible investment;

(i) advise the Governor and House of Assembly;

(j) coordinate responsible AI procurement by State MDAs;

(k) receive complaints within its jurisdiction;

(l) cooperate with Federal regulators and other stakeholders; and

(m) publish an annual report on the state of AI in Akwa Ibom State.

7. Composition

The Council shall consist of:

(a) a Chairperson appointed by the Governor;

(b) the Commissioner responsible for technology/digital economy

(c) the Commissioner responsible for Justice or the Commissioner's nominee

(d) the Commissioner responsible for Finance or the Commissioner's nominee

(e) the Director-General

(f) one AI/data-science expert

(g) one data-protection/privacy expert

(h) one cybersecurity expert

(i) one private-sector technology representative

(j) one consumer/digital-rights representative

(k) non-voting technical advisers as may be required.

8. Appointment, qualifications and tenure

(1) Non-ex officio members shall be appointed by the Governor subject to confirmation by the House of Assembly.

(2) Non-ex officio Members shall possess relevant qualifications and experience in artificial intelligence, data science, data protection, cyber security or another field relevant to the functions of the Council.

(3) A member shall hold office as prescribed by Statutory Boards Law of Akwa Ibom State.

9. Independence and conflicts of interest

(1) In regulatory and technical decisions, the Council shall act impartially, transparently and independently of improper influence in relation to the determination of a particular application, investigation, enforcement proceeding or other regulatory decision.

(2) A member or officer who has a direct or indirect personal, professional, financial or other interest in a matter before the council shall disclose the interest in writing and shall not participate in the consideration or determination of that matter.

10. Cessation and removal

A member ceases to hold office upon resignation, death, permanent incapacity, convicted of a felony or any offence involving dishonesty or corruption, bankruptcy where relevant, serious misconduct or lawful removal from office.

11. Meetings and quorum

The Council shall meet at least once every two months. Quorum shall be one-half of serving voting members, including the Chairperson or authorised presiding member.

12. Director-General

(1) The Governor shall appoint the Director-General subject to confirmation by the House of Assembly.

(2) The Director-General shall be the chief executive and accounting officer, responsible for administration and implementation.

13. Technical Evaluation Panel

The Council shall establish an AI Evaluation and Technical Assessment Panel comprising experts in AI, software engineering, cybersecurity, data protection, technology law, safety and relevant sectors. Detailed composition and procedures shall be prescribed by regulation.

14. Staff and consultants

The Council may employ staff and engage consultants subject to applicable public-service, procurement and financial laws, and may receive seconded personnel.

15. Training and capacity building

The Council shall support training for public officers, regulators, educators, entrepreneurs and other stakeholders in AI governance, safety, data protection, cybersecurity and responsible AI.

16. Regulations and guidelines

The Council may make regulations for the effective implementation of this Law. Technical standards, forms, assessment methodologies, reporting formats, sandbox procedures and other operational matters may be prescribed by regulation or guidelines.

PART III

RISK-BASED GOVERNANCE OF ARTIFICIAL INTELLIGENCE

17. Risk classification

AI systems shall be classified according to nature, scale, likelihood and severity of reasonably foreseeable harm, having regard to intended purpose and deployment context. The categories are Prohibited, High-Risk, Limited-Risk and Minimal-Risk.

18. Prohibited AI systems

(1) No person shall deploy, procure or operate within the scope of this Law an AI system or practice that—

(a) implements unlawful social scoring producing unjustified adverse treatment in unrelated contexts;
(b) materially manipulates or deceives a person, including by exploiting a known vulnerability, in a manner likely to cause serious harm;
(c) uses biometric identification or surveillance in a manner prohibited by applicable law;
(d) intentionally facilitates serious unlawful harm or violates fundamental rights in a manner prohibited by law; or
(e) is otherwise prescribed as prohibited after consultation with competent Federal authorities.

(2) An inaccurate or discriminatory AI system is not automatically prohibited; it may instead be subject to high-risk controls, remediation or suspension.

19. . High-risk AI systems

An AI system is high-risk where error, misuse or discriminatory outcome may significantly affect health, safety, fundamental rights, employment, education, access to essential services, critical infrastructure or other protected interests. Examples include high-impact recruitment, credit, healthcare, education, certain law-enforcement functions, critical infrastructure, border functions and safety-critical equipment.

20. High-risk obligations

Before deployment, an operator shall, as applicable—

1. Conduct an AI Impact Assessment;
2. Conduct a Data Protection Impact Assessment where required;

3. Implement risk-management and cybersecurity measures;
4. Ensure human oversight;
5. Maintain technical documentation and records;
6. Test accuracy, robustness, security and discriminatory outcomes;
7. Maintain incident reporting and shutdown mechanisms;
8. Monitor the system throughout its lifecycle; and
9. Register the system where required by regulation.

21. AI Impact Assessment

An AI Impact Assessment shall identify intended purpose, affected persons, data categories, foreseeable risks, discriminatory effects, cybersecurity threats, human oversight, mitigation measures and residual risks. The Council may prescribe proportionate templates.

22. Registration

The Council may establish a register of high-risk AI systems within the scope of this Law.

Registration is not a substitute for Federal or sector-specific approval. The Council may exempt low-scale or demonstrably low-impact deployments by regulation.

23. Limited-risk AI systems

Operators shall provide appropriate transparency, including disclosure where a person is interacting with AI or content has been substantially generated or altered by AI and that fact is material to understanding. Additional proportionate requirements may be prescribed for systems with heightened risks.

24. Minimal-risk AI systems

Minimal-risk systems shall generally not require registration under this Law, but remain subject to applicable privacy, consumer-protection, intellectual-property, cybersecurity and other laws.

25. Reclassification and appeal

The Council may reclassify a system where purpose, scale, functionality or risk changes. An affected operator shall receive written reasons and may appeal under Part VIII.

PART IV

RIGHTS, TRANSPARENCY AND RESPONSIBLE AI

26. Transparency

A deployer shall provide clear information about AI use where material to a person's interaction, decision or rights. High-risk systems shall provide proportionate information about purpose and principal decision factors.

27. Human oversight

High-risk AI shall have meaningful human oversight. A responsible human shall have sufficient authority, competence and information to intervene, override or stop the system where necessary.

28. Right to human review

A person materially affected by a fully or substantially automated decision concerning legal rights, employment, education, public services or another significant interest may request human review within the prescribed period.

29. Right to reasons and correction

Where a high-risk AI materially contributes to a significant adverse decision, the affected person shall, subject to lawful restrictions, receive an intelligible explanation and information on how to challenge the decision. A person may request correction of materially inaccurate personal information.

30. Fairness and non-discrimination

Operators shall take reasonable and proportionate measures to identify and mitigate unlawful discrimination and systematic bias in high-risk systems, including appropriate testing across relevant groups.

31. Accessibility and inclusion

Public-sector AI shall, where reasonably practicable, be accessible to persons with disabilities and usable by persons with different levels of digital literacy.

32. Complaints and redress

The Council shall establish an accessible complaints mechanism. Complainants shall receive outcomes and, where appropriate, remedies or referral to a competent regulator or court.

33. Trade secrets and security-sensitive information

Public disclosure of source code, proprietary information or security-sensitive information where disclosure would create disproportionate risk shall not be required, but the Council may require confidential access or independent audit where lawful and necessary.

PART V

DATA GOVERNANCE, PRIVACY AND CYBERSECURITY

34. Compliance with data-protection law

Processing of personal data in connection with AI shall comply with the Nigeria Data Protection Act 2023 and applicable regulations, guidelines and lawful directives. The Council shall cooperate with the Nigeria Data Protection Commission and shall not exercise its statutory powers.

35. Data governance

High-risk operators shall maintain appropriate measures concerning data quality, provenance, relevance, security, retention and lawful use. Privacy-by-design and data minimisation shall apply where required.

36. Data Protection Impact Assessment

Where AI processing is likely to result in high risk to natural persons, the operator shall conduct a Data Protection Impact Assessment where required by an Act of the National Assembly. The Council may require evidence of compliance or coordinate with the regulatory authority.

37. Cybersecurity

High-risk operators shall maintain proportionate cybersecurity controls including access control, logging, vulnerability management, incident response, backup and recovery, and security testing.

38. Serious AI incident reporting

An operator shall notify the Council of a serious AI incident within seventy-two hours of becoming aware of it, or within a shorter period prescribed for critical incidents, subject to coordination with Federal reporting obligations.

39. Data localisation and State data sovereignty

This Law shall not impose blanket State-level localisation of residents' personal data. For State Government systems involving sensitive or critical data, the Council may prescribe security, access, resilience, backup and approved-hosting requirements consistent with an Act of the National Assembly.

PART VI

ARTIFICIAL INTELLIGENCE IN GOVERNMENT

40. Responsible government use

Every State MDA deploying AI shall have a defined purpose, accountable owner, risk classification and proportionate safeguards. Legally significant public decisions shall not be delegated entirely to AI where human review is required by Law.

41. Government AI Register

The Council shall maintain a public register of material AI systems deployed by State MDAs, subject to lawful confidentiality and security restrictions.

42. Government AI Impact Assessment

Before deployment of a high-risk AI system, an MDA shall complete an AI Impact Assessment and satisfy applicable data-protection, cybersecurity and sectoral requirements.

43. Responsible AI procurement

High-risk AI procurement shall, where appropriate, include vendor due diligence, audit rights, data-use and ownership provisions, security, incident notification, human oversight, change management and termination rights.

44. Algorithmic accountability

Each MDA using high-risk AI shall designate an accountable officer responsible for compliance, monitoring and liaison with the Council.

45. Annual State of AI report

The Council shall publish an annual report covering government AI deployments, high-risk systems, incidents, complaints, enforcement, sandbox outcomes, investment, skills development and recommendations.

PART VII

REGULATORY SANDBOX AND INNOVATION

46. Establishment of sandbox

The Council shall establish a regulatory sandbox for controlled testing of innovative AI under enhanced supervision. Sandbox participation is not an exemption from applicable law; requirements may be proportionate to risk and scale.

47. Eligibility

Applicants shall be lawfully established or authorised in Nigeria, demonstrate innovation or public-interest value, provide risk and safeguard plans, demonstrate data-protection and cybersecurity measures, designate a responsible person, and not propose prohibited AI.

48. Safeguards and testing limits

The Council may impose user, geographic and time limits, disclosure, human oversight, data-isolation, reporting and shutdown conditions. Operators shall maintain a reliable means of stopping the system where necessary.

49. Monitoring

Sandbox participants shall submit periodic compliance and incident reports. The Council may conduct proportionate technical audits and inspections.

50. Exit pathways

At the end of a sandbox, the Council may grant State-level certification, a conditional extension, require remediation and testing, or direct cessation where material risks cannot be controlled.

51. Effect of State certification

Certification authorises operation only to the extent permitted by State law and does not confer nationwide approval or displace Federal or sector-specific requirements.

52. Innovation and local content incentives

Subject to appropriation and applicable fiscal and procurement laws, the State may provide grants, incubation, technical assistance, research partnerships and lawful procurement preferences, and may recommend eligible fiscal incentives to competent authorities.

PART VIII

COMPLIANCE, ENFORCEMENT AND APPEALS

53. Supervisory and investigative powers

The Council may request information, conduct or commission audits, require remedial measures, conduct lawful inspections and refer matters outside its jurisdiction to the competent regulatory authority.

54. Compliance notice

Where the Council reasonably believes there is a breach, it may issue a written notice specifying the breach, corrective measures and reasonable compliance period.

55. Administrative sanctions

Where authorised, the Council may impose warnings, remedial orders, administrative monetary penalties, restrictions, suspension or prohibition. Sanctions shall consider severity, duration, persons affected, intent or negligence, prior conduct, cooperation and remediation.

56. Offences

A person who knowingly deploys a prohibited AI system within the scope of section 18, obstructs a lawful investigation, knowingly submits materially false information, or intentionally conceals a serious AI incident commits an offence. AI regulation requires a different model because harm can arise from deployment of a prohibited system, failure to conduct a high-risk assessment, discriminatory outcomes, privacy violations, failure to disclose AI use, or failure to comply with an enforcement notice.

(1) A person who contravenes a provision of this Law for which no specific penalty is prescribed commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine not exceeding ₦5,000,000 or confinement for a term not exceeding two years, or to both

(b) in the case of a body corporate, to a fine not exceeding ₦20,000,000.

(2) A person who knowingly develops, deploys, supplies, markets, makes available or uses a Prohibited AI System in contravention of this Law commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine of not less than ₦20,000,000 or confinement for a term not exceeding five years, or to both

(b) in the case of a body corporate, to a fine of not less than ₦50,000,000 or an amount equivalent to 3% of its annual turnover in Nigeria for the preceding financial year, whichever is higher.

(3) Where an offence under subsection (2)—

(a) causes death, serious bodily injury or substantial physical harm

(b) causes significant financial loss to affected persons

(c) involves systematic discrimination or denial of fundamental rights

(d) involves the deliberate manipulation or exploitation of children or other vulnerable persons

(e) is committed for financial gain or other unlawful benefit

(f) affects a critical public service or public infrastructure

(g) is committed repeatedly or after a lawful enforcement or prohibition notice,

the offender is liable on conviction—

(i) in the case of an individual, to a fine of not less than ₦50,000,000 or confinement for a term of five to ten years, or to both

(ii) in the case of a body corporate, to a fine of not less than ₦100,000,000 or 5% of its annual turnover in Nigeria for the preceding financial year, whichever is higher.

(4) A provider or deployer of a High-Risk AI System who knowingly—

(a) deploys the system without the required risk assessment

(b) fails to implement prescribed human oversight

(c) fails to maintain required technical documentation or records

(d) fails to conduct required testing, monitoring or impact assessment

(e) fails to implement required cybersecurity or risk-management measures

(f) knowingly deploys a materially non-compliant system

(g) continues to deploy the system after a lawful suspension or prohibition, commits an offence and is liable on conviction—

(i) in the case of an individual, to a fine of not less than ₦5,000,000 and not exceeding ₦20,000,000, or confinement for a term not exceeding three years, or to both

(ii) in the case of a body corporate, to a fine of not less than ₦20,000,000 and not exceeding ₦50,000,000.

(5) A provider or deployer of a Limited-Risk AI System who knowingly fails to comply with applicable transparency, disclosure, labelling or user-notification requirements commits an offence and is liable—

(a) in the case of an individual, to a fine not exceeding ₦2,000,000

(b) in the case of a body corporate, to a fine not exceeding ₦10,000,000.

(c) where the contravention is corrected promptly following a compliance notice, the Commission may impose an administrative sanction instead of criminal prosecution.

(6) A person shall not be liable to a criminal penalty merely for developing, deploying or using a Minimal-Risk AI System. However, where the use of such a system constitutes fraud, discrimination, unlawful processing of personal data, cybercrime or another offence under Nigerian law, the person shall be liable under the applicable law.

(7) A person who knowingly provides false, incomplete or materially misleading information to the Council, an auditor, an authorised officer or another competent regulatory authority in connection with an AI system commits an offence and is liable on conviction—

(a) to a fine of not less than ₦5,000,000 and not exceeding ₦20,000,000 in the case of an individual

(b) to a fine of not less than ₦20,000,000 and not exceeding ₦50,000,000 in the case of a body corporate.

(8) A person who fails to comply with a lawful compliance, remediation, suspension or prohibition notice issued under this Law commits an offence and is liable—

(a) in the case of an individual, to a fine not exceeding ₦10,000,000 or confinement for a term not exceeding two years, or to both; and

(b) in the case of a body corporate, to a fine not exceeding ₦50,000,000.

(c) where the contravention continues after the expiration of the compliance period, the Council may impose an additional administrative penalty of up to ₦500,000 for each day the contravention continues.

(9) A person shall not knowingly create, generate, manipulate, alter or materially transform an image, video, audio recording or other digital content through the use of an Artificial Intelligence System or other synthetic media technology where the person intends that the resulting content-

(a) falsely represent a real person as having said, done or participated in an act or event which did not occur;

(b) deceive or defraud any person;

(c) impersonate another person for an unlawful purpose;

(d) cause reputational, financial or other material harm to another person;

(e) incite violence, hatred, public disorder or unlawful conduct;

(f) threaten, intimidate, blackmail or harass another person; or

(g) otherwise cause malicious harm through deliberate deception.

(h) A person who knowingly publishes, uploads, transmits, distributes, sells, advertises, shares or causes to be distributed a deepfake or materially manipulated synthetic media content described in subsection (1) commits an offence where the person knows, or ought reasonably to know, that the content is materially false or misleading and is being disseminated for a prohibited purpose.

(i) A person shall not be liable under this section solely because the person creates or distributes synthetic or manipulated content for—

(i) legitimate artistic, dramatic or entertainment purposes;

(ii) satire or parody, where the content is reasonably identifiable as satire or parody and is not used for a prohibited purpose;

(iii) bona fide academic, scientific, technological or research purposes; or

(iv) legitimate journalism or public-interest communication undertaken without intent to deceive or cause prohibited harm.

(v) Where the content referred to in this section relates to an identifiable public officer, political candidate, public institution, election, public emergency, critical infrastructure or other matter of substantial public interest, the court may consider the potential for widespread public harm in determining the appropriate penalty.

(10) A person commits an offence under this Law where, whether physically present within or outside Akwa Ibom State, where the person knowingly—

(a) creates, commissions, generates or materially manipulates AI-generated or synthetic content;

(b) publishes, transmits, distributes or causes the content to be distributed; or

(c) directs, facilitates or procures another person to undertake any of the acts specified in paragraphs (a) or (b) where—

(i) the content is specifically targeted at a person, community, institution, business, public institution, public process, infrastructure or activity within Akwa Ibom State; and

(ii) the person intends, or reasonably foresees, that the content will cause deception, fraud, intimidation, harassment, reputational injury, public disorder, violence, financial loss or other malicious harm within the State.

(d) For the purposes of subsection (1), an offence shall be deemed to have a sufficient territorial connection with Akwa Ibom State where—

(i) the intended or actual victim is ordinarily resident or located in the State;

(ii) the targeted institution, business or infrastructure is located in the State;

(iii) the content is specifically directed at an audience within the State;

(iv) the harmful consequences substantially occur within the State; or

(v) the person uses a digital service, platform, infrastructure or network to deliberately target persons or activities within the State.

(e) nothing in this section shall be construed as conferring upon the State any jurisdiction contrary to the Constitution of the Federal Republic of Nigeria or any applicable Act of the National Assembly.

(f) Where a person suspected of an offence under this section is located outside Akwa Ibom State, the relevant State institution may, subject to applicable Law, cooperate with competent Federal regulatory authorities and other competent domestic or foreign authorities for investigation, preservation of evidence, identification of the perpetrator and enforcement of any lawful order.

(11) A person convicted of an offence under the provisions relating to malicious deepfake creation or dissemination shall be liable to—

(a) in the case of an individual, a fine of not less than ₦10,000,000 or confinement for a term not exceeding three years, or both; and

(b) in the case of a corporate body or other incorporated entity, a fine of not less than ₦25,000,000, in addition to any applicable administrative sanctions.

(c) where the offence—

(i) results in financial loss;

(ii) causes serious reputational injury;

(iii) facilitates fraud or identity theft;

(iv) causes or materially contributes to violence or public disorder;

(v) targets a public institution or critical infrastructure;

(vi) is committed for financial gain; or

(vii) involves the deliberate dissemination of the content to a substantial number of persons, the court may impose an enhanced fine of up to ₦50,000,000 for an individual and ₦100,000,000 for a corporate body, or such higher amount as may be prescribed by regulations.

(d) where a person convicted under this section derived financial benefit from the offence, the court may order—

(i) forfeiture of the proceeds of the offence;

(ii) restitution or compensation to the victim;

(iii)removal, disabling or correction of the offending content where legally practicable;

(iv) preservation or disclosure of relevant digital evidence in accordance with law; and

(v) any other appropriate remedy permitted by law.

(e) where an offence is committed by a corporate body with the consent, connivance or neglect of a director, manager, secretary or other principal officer, that officer shall be liable to prosecution under this section in addition to the liability of the corporate body.

(f) nothing in this section shall prevent the prosecution of a person under any other applicable law where the conduct also constitutes an offence under that law.

(12) Where the financial benefit obtained, or loss avoided, as a result of an infringement exceeds the applicable maximum fine prescribed under this section, the Court or may impose a penalty of up to three times the value of the benefit obtained or loss avoided, subject to applicable law.

(13) In addition to any fine or imprisonment imposed under this section, the Court may -

(a) order restitution or compensation to persons affected by the unlawful AI deployment;

(b) order the refund of monies obtained through the unlawful deployment;

(c) order the destruction, disabling or withdrawal of an unlawful AI system;

(d) order the deletion, correction or preservation of data where legally appropriate;

(e) order the suspension of an AI system for a specified period; or

(f) make any other order necessary to prevent continuing harm.

(14) Where an offence under this Law is committed by a body corporate, any director, manager, partner, beneficial owner or senior officer who knowingly authorised, permitted, participated in or facilitated the commission of the offence commits the offence and is liable to the applicable penalty.

(a) a person shall not be liable under this subsection where the person establishes that the offence occurred without that person's knowledge, consent or connivance and that the person exercised reasonable diligence to prevent its commission.

(15) In determining the appropriate administrative or criminal penalty, regard shall be had to—

(a) the nature, seriousness and duration of the infringement

(b) the purpose and risk classification of the AI system

(c) the number of persons affected

(d) the severity and duration of the harm

(e) whether fundamental rights were affected

(f) whether the conduct was intentional, reckless or negligent

(g) the financial benefit obtained or loss avoided

(h) the size, turnover and financial capacity of the offender

(i) whether the offender voluntarily reported the infringement

(j) steps taken to mitigate or remedy the harm

(k) previous violations

(l) whether the offender is a start-up, small or medium-sized enterprise.

(16) Without prejudice to criminal prosecution, the Council may impose one or more of the following administrative sanctions—

(a) written warning

(b) compliance or remediation order

(c) requirement to conduct an independent AI audit

(d) requirement to undertake an AI impact assessment

(e) restriction on deployment

(f) suspension of deployment

(g) withdrawal or cancellation of a State certification or registration

(h) administrative monetary penalty

(i) prohibition on deployment of the AI system within the State

(j) referral to another competent regulatory or law-enforcement authority.

(17) Before imposing a final administrative sanction, the Authority shall give the affected person—

(a) written notice of the alleged contravention;

(b) reasonable opportunity to make representations;

(c) reasons for the proposed sanction; and

(d) information concerning the right of appeal.

Except where immediate action is reasonably necessary to prevent imminent and serious harm, no final sanction shall be imposed without an opportunity to be heard.

(18) A person affected by a final administrative decision under this section may appeal in accordance with the appeal procedure established under this Law. Nothing in this section shall prevent a person from seeking judicial review or any other remedy available under Nigerian law.

(19) Where the same conduct constitutes an offence or infringement under another applicable Nigerian Law, the Council shall cooperate with the relevant regulatory or law-enforcement authority and shall take into account any penalty, compensation, forfeiture or other sanction already imposed in respect of the same conduct, so as to avoid disproportionate or duplicative punishment.

(20) Nothing in this section shall—

(a) limit the powers of a competent Federal regulatory authority

(b) prevent prosecution under an Act of the National Assembly

(c) confer on the State jurisdiction over a matter constitutionally reserved to the Federal Government

(d) constitute a State certification or approval as a substitute for any Federal licence, registration or approval

57. Emergency suspension

Where an AI system presents an imminent and serious risk to health, safety or fundamental rights, the Council may issue an emergency suspension or cessation order, subject to prompt review and the right to be heard.

58. Right to be heard

Before a final adverse order, the Council shall give notice of proposed action, reasons and a reasonable opportunity to make representations, except where immediate interim action is necessary to prevent serious harm.

59. Administrative appeal

A person dissatisfied with a final decision may appeal to an Appeals Committee designated by the Council within fourteen business days or such longer period as may be allowed for good cause. The Committee shall be independent of the original decision-maker.

60. Judicial review

Nothing in this Law limits judicial review or any remedy available under the Constitution or any applicable law. Nothing in this Law shall oust the jurisdiction of a court.

PART IX

FINANCIAL PROVISIONS, REPORTING AND ACCOUNTABILITY

61. Fund of the Council

The Council shall maintain a fund comprising appropriations, lawful grants and donations, lawful fees and charges, income from services and other lawful receipts.

62. Fees and charges

(1) The model recommended is a cost-recovery and risk-based fee framework, where basic registration is relatively affordable, high-risk assessment costs more, large companies pay more than SMEs, and innovation/sandbox participation should be free or heavily subsidised for start-ups and SMEs. Considerations should be made to SME size and market size when setting conformity-assessment fees.

(2) The Council may, subject to regulations made under this Law, prescribe reasonable fees and charges for services provided under this Law, including—

(a) registration of AI developers, providers or deployers where registration is required;

(b) certification or approval of High-Risk AI Systems;

(c) conformity assessment or independent technical assessment;

(d) review of AI impact assessments;

(e) registration or renewal of approved AI systems;

(f) applications for regulatory sandbox participation;

(g) technical audits, testing or verification undertaken by or on behalf of the Council;

(h) accreditation or recognition of AI assurance, testing or conformity-assessment bodies;

(i) applications for amendments to an existing registration, certification or approval

(j) any other regulatory or technical service reasonably provided under this Law.

(3) In prescribing fees under subsection (1), the Council shall ensure that fees are—

(a) reasonable and proportionate to the regulatory service provided;

(b) transparent and publicly published;

(c) based, as far as practicable, on the actual or reasonably estimated cost of providing the service;

(d) proportionate to the risk, complexity and scale of the AI system;

(e) reviewed periodically to take account of inflation and changes in the cost of regulation

(f) structured so as not to create an unreasonable barrier to innovation or market entry.

(4) The Council shall establish different fee categories for—

(a) Minimal-Risk AI Systems

(b) Limited-Risk AI Systems

(c) High-Risk AI Systems

(d) other AI systems or activities designated by regulation.

(5) Subject to adjustment by regulation, the following initial maximum fees shall apply:

Service	Recommended Maximum Fee
Minimal-Risk AI registration, where applicable	₦25,000
Limited-Risk AI registration	₦100,000
High-Risk AI registration	₦500,000
High-Risk AI conformity/technical assessment application	₦1,000,000
AI impact assessment review	₦500,000

Service	Recommended Maximum Fee
Registration renewal	50% of applicable initial fee
Material modification/re-certification	50% of applicable assessment fee
Regulatory sandbox — SME/start-up	No application fee
Regulatory sandbox — large enterprise	Cost-recovery basis
Accreditation of AI assurance/testing body	₦500,000
Independent technical audit requested by the Council	Actual reasonable cost

(6) The fees prescribed under subsection (4) may be varied by regulations made under this Law, provided that the Council shall publish the applicable fee schedule before the fees take effect.

(7) No fee shall be payable for registration, assessment or participation where the Council determines that the AI system is being developed or deployed—

(a) solely for academic research;

(b) by a public educational institution for non-commercial research;

(c) for a public-interest or humanitarian purpose;

(d) as part of a government-approved innovation programme; or

(e) within an approved regulatory sandbox, where the participant qualifies for a fee exemption under this Law.

(8) The Council shall provide reduced fees, payment flexibility or fee waivers for eligible small and medium-sized enterprises and start-ups.In determining eligibility, the Council shall consider—

(a) annual turnover;

(b) number of employees;

(c) age of the enterprise;

(d) scale of deployment;

(e) number of affected users;

(f) risk classification of the AI system; and

(g) whether the AI system is being developed for research, experimentation or commercial deployment.

(9) Participation in an AI regulatory sandbox shall be free of charge for eligible SMEs, start-ups, academic institutions and public-interest projects.The Council may recover exceptional costs incurred in connection with a sandbox project where such costs—

(a) are directly attributable to the project;

(b) are reasonable and properly documented; and

(c) have been disclosed to the participant before the costs are incurred.

(d) a large commercial enterprise may be charged a reasonable participation fee based on the cost of providing the sandbox services.

(10) Where the Council requires an independent conformity assessment, technical audit, penetration test, algorithmic assessment or other specialist evaluation, the cost of the assessment shall ordinarily be borne by the provider or deployer of the AI system. The Council shall ensure that—

(a) the service provider is appropriately qualified;

(b) fees are reasonable and transparent;

(c) there is no conflict of interest; and

(d) SMEs and start-ups are not subjected to disproportionate assessment costs.

(11) The Council may prescribe an annual regulatory fee for registered providers or operators of High-Risk AI Systems.The annual fee shall be based on one or more of—

(a) risk classification;

(b) number of AI systems registered;

(c) scale of deployment;

(d) number of affected users;

(e) complexity of the system; and

(f) size and turnover of the operator.

(12) No Fee for Ordinary AI Use and nothing in this section shall require a person to pay a fee merely because that person—

(a) uses a commercially available AI tool for ordinary personal purposes;

(b) uses AI for ordinary office, educational or professional productivity;

(c) develops open-source AI software for non-commercial purposes; or

(d) conducts lawful AI research that does not fall within a regulated activity under this Law.

(13) The Authority shall publish on its website and through other appropriate channels—

(a) the applicable fees;

(b) the basis upon which each fee is calculated;

(c) eligibility criteria for exemptions and reductions;

(d) payment procedures;

(e) processing timelines; and

(f) procedures for requesting a review or waiver.

No fee shall be payable unless it has been properly prescribed and published.

(14) The Authority may, on application, reduce, defer or waive a fee where it is satisfied that—

(a) payment would create undue hardship;

(b) the applicant is an eligible start-up or SME;

(c) the AI system serves an important public-interest purpose;

(d) the project is primarily research-oriented; or

(e) the waiver would promote innovation consistent with the objectives of this Law.

(15) All fees collected under this Law shall be applied in accordance with applicable public-finance laws and may, subject to appropriation and applicable financial controls, support—

(a) AI regulatory supervision;

(b) technical testing and assessment;

(c) cybersecurity capability;

(d) AI regulatory sandboxes;

(e) public awareness and education;

(f) AI research and innovation;

(g) training and capacity development; and

(h) development of regulatory standards and technical infrastructure.

(16) The Council shall review the fee structure at least once every three years and may recommend amendments where necessary to reflect—

(a) inflation;

(b) changes in technology;

(c) the cost of regulatory supervision;

(d) changes in the number and complexity of regulated AI systems;

(e) international regulatory developments; and

(f) the economic impact of the fees on Nigerian businesses and innovation.

63. Accounts and Audit

The Council shall keep proper accounts and ensure annual audit in accordance with applicable State public-finance and audit laws.

64. Annual Estimates

The Council shall prepare annual estimates of income and expenditure and submit them through the appropriate State regulatory in accordance with applicable public-finance laws.

65. Annual report and legislative oversight

The Council shall submit an annual report to the Governor and House of Assembly, including audited accounts, regulatory activity, enforcement, incidents, government deployments, sandbox outcomes and recommendations.

66. Gifts, grants and procurement

The Council may accept lawful gifts and grants that are consistent with its functions and do not create conflicts of interest. Procurement and expenditure shall comply with applicable State laws.

PART X

MISCELLANEOUS

67. Confidentiality

Members, officers, consultants and persons acting for the Council shall protect confidential information and disclose it only as authorised by law. Lawful disclosure to a competent regulator, court or public authority is permitted.

68. Immunity and indemnity

No member or officer is personally liable for an act or omission done in good faith in lawful discharge of official functions, without prejudice to liability for fraud, corruption, bad faith or other unlawful conduct.

69. Service of notices

A notice under this Law may be served electronically or by another lawful means prescribed by regulation, provided there is reasonable evidence of delivery.

70. Judgments and public funds

Enforcement of judgments against the Council shall be governed by applicable law. Nothing in this Law shall create an unlawful immunity from execution.

71. Regulations and standards

Regulations may address risk classification, registration, certification, AI Impact Assessments, technical documentation, incident reporting, government procurement, sandbox administration, fees, administrative sanctions and other matters necessary for implementation.

72. Review of the Law

The Council shall, not later than three years after commencement and every three years thereafter, review the operation of this Law and report to the House of Assembly, considering technological developments, Acts of the National Assembly and policies, regulatory experience, innovation outcomes, economic impact and protection of rights.

73. Transitional provisions

Lawful AI activities existing at the commencement of this Law shall be given a reasonable transition period prescribed by regulation, except where immediate action is required to prevent serious harm.

74. Savings

Nothing in this Law shall invalidate or affect any approval, licence, contract, intellectual-property right, obligation, offence, penalty or liability created under the Act of the National Assembly.

75. Interpretation

AI system means a machine based system that processes inputs to generate predictions, content, recommendations or decisions capable of influencing physical or virtual environments.

Council means the Akwa Ibom State Artificial Intelligence Council

Provider/developer means a person or entity that develops or makes an AI sytem available; developer means a person or entity using an AI system under its authority

High Risk AI system means an AI system which by intended purpose or reasonably foreseeable use, presents significant risk to health, safety, fundamental rights, emplyment, education, access to essential services or other legally protected interests

Prohibited AI system means an AI system or use expressly prohibited under this Law

AI impact assessment means a documented assessment of risks, impacts and safeguards associated with an AI system

Serious AI incident means an event involving an AI system that causes or creates a significant risk of causing death, serious injury, substantial unlawful discrimination, major privacy harm, material cybersecurity compromise or significant disruption of an essential service

Personal data has the meaning assigned under applicable data Protection legislation

Human oversight means meaningful human ability to monitor, intervene in, override or stop an AI system

76. Short Title

This Law may be cited as the Akwa Ibom State Artificial Intelligence Governance, Development and Responsible Adoption Law, 2026.

SCHEDULE

SCHEDULE 1

Regulatory Framework and risk categorization

1. Prohibited Systems are systems considered unacceptably harmful and are hereby banned and prohibited from deployment. These include :

i. Social scoring systems that rank citizens based on their behaviour and use the score to determine access to essential services.
ii. AI that manipulates people's behaviour in ways that cause significant harm, particularly by exploiting vulnerable groups such as children.
iii. AI systems used for indiscriminate mass biometric surveillance in circumstances where the law prohibits such use.
iv. AI designed to make decisions that unfairly discriminate against people based on protected characteristics.
v. AI systems used to infer highly sensitive personal characteristics without a legitimate legal basis.
vi. Certain forms of autonomous AI used to cause serious physical harm or violate fundamental human rights.

2. High-Risk Systems that can have serious consequences on health, safety, rights, employment, education or access to essential services and are to be strictly controlled by the regulatory authority through testing, monitoring and human oversight. They include:

i. AI used in healthcare to diagnose diseases or recommend major treatments.

ii. AI used in recruitment and employment to select or reject job applicants.

iii. AI used by banks to determine creditworthiness or loan eligibility.

iv. AI used in education to determine admission, assessment or progression of students.

v. AI used in law enforcement, such as systems assisting with certain criminal investigations or risk assessments.

vi. AI controlling critical infrastructure, such as electricity, water or transportation systems.

vii. AI used in border control and immigration to assess individuals.

viii. AI incorporated into medical devices, aircraft, vehicles or industrial machinery where failure could threaten safety.

3. Limited-Risk Systems generally present lower risks,developers must inform users that they are interacting with AI or that AI-generated content is being used. They include:

i. AI chatbots used for customer service.

ii. Virtual assistants that answer routine questions.

iii. AI systems that generate marketing content.

iv. AI tools that generate or edit images, audio or video.

v. AI systems used to make recommendations, such as suggesting products or entertainment.

vi. AI-powered translation tools.

vii. AI systems used to summarize documents or generate routine business correspondence.

4. Minimal-Risk Systems pose little or no significant risk to individuals or society and generally require few or no special regulatory obligations. They include:

i. AI used in **video games** to control non-player characters.

ii. Spam filters in email applications.

iii. AI-powered **music or movie recommendations**.

iv. Computer vision used to organize personal photographs.

v. AI used for basic grammar and spelling suggestions.

vi. AI used to improve image quality or remove background noise.

vii. AI used for routine inventory forecasting where it does not make consequential decisions about people.

Risk category	Main characteristic	Examples
Prohibited	Unacceptable risk; deployment/use is banned	Social scoring, certain manipulative or abusive surveillance systems
High-risk	Significant potential impact on safety or fundamental rights	Recruitment, credit, healthcare, education, critical infrastructure
Limited-risk	Some transparency or disclosure obligations may apply	Chatbots, AI-generated content, customer-service AI
Minimal-risk	Little potential for significant harm	Video-game AI, spam filters, photo organization

5. Data Governance and Privacy Rights

(1) Operators of high-risk AI systems (including facial recognition in public spaces, automated critical hiring, and judicial sentencing aids) must submit an annual Algorithmic Impact Assessment (AIA) to the Council.

(2) AI training models processing biometric or genomic data of Akwa Ibom residents must store a secure, audited registry copy locally in compliance with the Nigeria Data Protection Act.

(3) Every citizen of Akwa Ibom State has the right to request a human review of any fully automated decision that significantly impacts their legal rights, employment, or access to public utilities.

SCHEDULE 2

Miscellaneous

1. Sandbox and Innovation Subsidies

The Ministry of Science and Technology shall establish an AI Regulatory Sandbox to permit startups to test innovative models under relaxed compliance conditions for up to 12 months.

2. Eligibility Criteria for Sandbox Entry

(a) To enter the Sandbox, an applicant must satisfy all of the following requirements:

i. Local Incorporation: The entity must be registered with Nigeria's Corporate Affairs Commission (CAC). Its principal place of business or an active operations hub must be in Akwa Ibom State.

ii. Innovative Threshold: The AI application must use generative models, neural networks, or automated workflows that solve local problems in agriculture, healthcare, finance, education, or public service.

iii. Risk Assessment: The system must not fall into the *Prohibited AI* category (such as predatory social scoring or covert biometric surveillance).

iv. Consumer Protection Blueprint: The applicant must show a basic plan to protect consumer data and prevent algorithmic bias.

3. Safeguards, Testing Limits, and Guardrails

(a) while operating inside the Sandbox, developers must adhere to strict operational boundaries to prevent widespread public harm:

i. Capped User Base: Sandbox participants can deploy their software to a maximum of 10,000 active users within the state during the trial period.

ii. Informed Consent Mandate: Every user interface must display a prominent, clear notification stating: *"This service is running inside the Akwa Ibom State AI Regulatory Sandbox. Automated systems are currently undergoing safety evaluations.*

iii. Data Localization & Isolation: All user-tested datasets must be hosted on secure, isolated cloud instances or local state servers. They cannot be shared with third-party global models without encryption.

iv. The "Kill Switch" Protocol: Operators must maintain an absolute manual override (kill switch). This allows the developer or the Council to shut down the system instantly if it generates malicious content, exhibits severe algorithmic bias, or leaks private data.

4. Exit Pathways and Post-Sandbox Certification

(a) at the end of the 12-month window, the entity must transition out of the Sandbox via one of three structural pathways:

(i) standard Compliance Certification: Granted to systems that pass all safety, fairness, and data audits. The Council issues a *Certificate of Algorithmic Compliance*. This unlocks full commercial deployment rights across Nigeria.

(ii) conditional Extension: Granted if the tech is highly viable but its risk profile requires more monitoring. The Council may grant a one-time, 6-month extension with specific testing limits.

(iii) mandatory Cease and Desist: Applied if the system fails to fix critical vulnerabilities, shows persistent bias, or violates privacy limits during the trial. The system is barred from operating within Akwa Ibom State.

---

5. Regulatory Incentives for Local Startups

(a) to encourage compliance and support the local tech ecosystem, the State provides three distinct incentives to Sandbox participants:

i. Zero Registration Fees: Total exemption from all initial AI registration, processing, and auditing fees during the 12-month sandbox period.

ii. Procurement Preference: Startups that graduate with a *Certificate of Algorithmic Compliance* get priority consideration under the Akwa Ibom State Public Procurement rules for government digital upgrades.

iii. Tax Holiday Alignment: Successful completion of the program gives startups a formal recommendation to the Akwa Ibom State Internal Revenue Service (AKIRS) for a 2-year state-level tax holiday on corporate tech income.

iv.

SCHEDULE 3

REGULATIONS

Rule 1: Composition and Convening of the Evaluation Panel

1. The Panel: The Council shall empanel an AI Evaluation and Technical Assessment Panel (hereinafter referred to as "the Panel") comprising five (5) members:
    i. The Director of Technical Standards (Chairperson).
    ii. One (1) Senior Software Engineer or Data Scientist with expertise in neural networks.
    iii. One (1) Legal Practitioner specializing in technology law and data privacy.
    iv. One (1) Cybersecurity expert certified in algorithmic auditing.
    v. One (1) representative of the Akwa Ibom State Ministry of Science and Technology.
2. Quorum: The quorum for any evaluation session, hearing, or technical review shall be three (3) members, which must include the Chairperson and either the Legal Practitioner or the Cybersecurity expert.
3. Sittings: The Panel shall sit at least once every month at the Council's Headquarters in Uyo, or virtually via secure digital video-conferencing channels as designated by the Chairperson.

Rule 2: The Application and Intake Process

1. Submission of Application: Every developer or deployer seeking entry into the Regulatory Sandbox or requesting standard compliance certification shall submit a formal digital application through the official Council portal.
2. Required Documentation: The applicant must provide an AI System Transparency Dossier containing:
    i. Complete description of the machine learning architecture, model types, and data pipelines.
    ii. A Data Protection Impact Assessment (DPIA) aligning with Nigeria Data Protection Act (NDPA) regulations.
    iii. Source code access protocols for auditing or simulated architectural tests.
    iv. A detailed description of human-in-the-loop fallback mechanisms and the "Kill Switch" architecture.
3. Acknowledge and Timelines: The Secretariat shall acknowledge receipt of the application within forty-eight (48) hours. The Panel must issue a preliminary decision on admissibility within fourteen (14) business days.

Rule 3: Technical Evaluation and Auditing Protocols

1. The Review Method: The Panel shall subject the candidate AI system to an algorithmic evaluation focusing on three core criteria:
    i. Bias and Fairness Check: Testing the system using localized Akwa Ibom demographic variations to prevent gender, ethnic, or socioeconomic algorithmic discrimination.
    ii. Security and Robustness: Stress-testing the model against data poisoning, adversarial cyber attacks, and structural system failures.
    iii. Data Governance and Isolation: Confirming that citizen training sets are properly sandboxed, anonymized, and stored in secure localized instances.
2. Request for Clarification: The Panel may issue a written *Notice to Clarify* requiring the applicant to explain technical anomalies within seven (7) business days. Failure to respond or comply satisfies grounds for automatic rejection of the application.

Rule 4: Sandbox Monitoring and Reporting Procedures

1. Monthly Logs: Operators admitted into the 12-month Sandbox must submit automated compliance logs to the Panel on the first business day of every month.
2. Content of Logs: Logs must explicitly report:
    i. The unique count of active users within Akwa Ibom State (verifying it remains below the 10,000-user cap).
    ii. A record of all manual overrides or activations of the human-in-the-loop fallback protocols.
    iii. Documented instances of system errors, data anomalies, or security breaches.
3. Spot Inspections: The Panel reserves the right to execute unannounced digital audits or physical facility inspections at the developer's registered Akwa Ibom business premises.

Rule 5: Hearing and Determination Procedures

1. The Right to Be Heard: Where the Panel intends to revoke sandbox status or deny compliance certification, it shall issue a *Notice of Intent to Refuse* to the applicant.
2. Oral Representation: The applicant has seven (7) business days from the receipt of the Notice to request an administrative hearing before the Panel to defend their model.
3. Decisions: Decisions of the Panel shall be determined by a simple majority vote of the sitting members. In the event of a tie, the Chairperson shall hold a casting vote. All final

orders must be signed by the Chairperson, issued in writing, and served to the applicant within three (3) business days of voting.

Rule 6: Appeals and Judicial Recourse

1. Administrative Appeal: Any applicant dissatisfied with a final decision of the Panel may file an administrative appeal to the full Board of the Council within fourteen (14) business days.
2. Judicial Appeal: If the applicant remains dissatisfied with the Board's decision, they may file an application for Judicial Review at the High Court of Akwa Ibom State within thirty (30) days of receiving the Board’s final decision, in accordance with the High Court Civil Procedure Rules.