AKWA IBOM STATE HOUSE OF ASSEMBLY

AKWA IBOM STATE AUGMENTED REALITY, VIRTUAL REALITY, AND SPATIAL COMPUTING PROTECTION BILL, 2026

A BILL

FOR A LAW TO PROVIDE FOR THE RESPONSIBLE DEVELOPMENT, DEPLOYMENT, GOVERNANCE AND USE OF AUGMENTED REALITY, VIRTUAL REALITY AND SPATIAL COMPUTING TECHNOLOGIES IN AKWA IBOM STATE; TO ESTABLISH RIGHTS RELATING TO VIRTUAL SPATIAL PRIVACY AND BIOLOGICAL TELEMETRY; TO PROTECT CITIZENS AGAINST UNAUTHORISED SPATIAL TRACKING, PROFILING AND DIGITAL INTRUSION; TO PROVIDE FOR THE RESPONSIBLE CREATION AND USE OF DIGITAL TWINS OF PUBLIC INFRASTRUCTURE AND HERITAGE ASSETS; TO PROMOTE LOCAL IMMERSIVE DIGITAL CONTENT, EDUCATION, RESEARCH AND INNOVATION; 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.(Barr) Prince Ukpong Akpabio

Hon. Jerry Otu

Hon. Prince Aniefiok Attah

Hon. Bassey Pius Bassey

Arrangement of Sections

PART I

Preliminary Provisions

1. Objectives
2. Application and Scope
3. Guiding Principles

PART II

Institutional And Regulatroy Framework

4. Establishment of the Akwa Ibom Spatial Computing and Immersive Technology Council
5. Functions of the Council
6. Composition of the Council
7. Appointment and Tenure of Members
8. Technical and Advisory Panels
9. Meetings and Quorum
10. Secretariat and Staff
11. Regulatory Guidelines and Standards

PART III

Virtual Spatial Provacy And Biological Telemetry

12. Right to Virtual Spatial Privacy
13. Definition of Biological Telemetry
14. Classification of Spatial and Biological Data
15. Consent for Collection of Biological Telemetry
16. Prohibition of Covert Telemetry Collection

17. Purpose Limitation and Data Minimisation
18. Prohibition of Unauthorised Sale or Trading of Telemetry
19. Retention and Deletion of Telemetry
20. Right of Access, Correction and Withdrawal
21. Profiling and Behavioural Inference
22. Children's Virtual Spatial Privacy

PART IV

Immersive Systems Safety And Consumer Protection

23. Transparency Requirements
24. Safety-by-Design
25. Immersive Content Disclosures

26. Manipulative or Deceptive Immersive Experiences
27. Spatial Harassment and Digital Intrusion
28. Protection Against Unauthorised Recording
29. Accessibility and Inclusion
30. Consumer Complaints and Redress
31. Platform Accountability

PART V

Digital Twins, Spatial Mapping And State Heritage

32. Regulation of Public Digital Twins
33. Digital Twin Clearance
34. Mapping of State Infrastructure

35. Digital Replication of Heritage Assets
36. Cultural and Heritage Data Register
37. Commercial Exploitation of State Digital Twins
38. Attribution and Benefit-Sharing
39. Exceptions for Education, Research and Public Interest
40. Security of Critical Spatial Models

PART VI

Data Governance, Cybersecurity And Spatial Security

41. Spatial Data Governance
42. Cybersecurity Requirements
43. Protection Against Spatial System Hijacking

44. Encryption and Access Controls
45. Incident Reporting
46. Data Storage and Cross-Border Transfers
47. Audit Trails and Technical Records

PART VII

Education, Innovation And Local Content

48. Immersive Technology Regulatory Sandbox
49. Eligibility for Sandbox Participation
50. Sandbox Safeguards and Testing Limits

51. Exit Pathways and Certification
52. Educational AR/VR Content Development
53. Local Immersive Content Incentives
54. Research and Development Exemptions
55. Skills Development and Local Capacity
56. Public-Private Partnerships

PART VIII

Offences, Penalties And Remedies

57. Unlawful Collection of Biological Telemetry
58. Unauthorised Sale or Disclosure of Telemetry
59. Unlawful Spatial Tracking and Profiling
60. Spatial Harassment and Digital Intrusion
61. Unauthorised Digital Twin Replication

62. Fraudulent or Deceptive Immersive Services
63. Cybersecurity Violations
64. Corporate Liability
65. Continuing Offences
66. Administrative Sanctions
67. Compensation and Civil Remedies
68. Appeals and Judicial Review

PART IX

Finance, Fees And Miscellaneous

69. Fees and Charges
70. Funding of the Council
71. Accounts and Audit
72. Annual Report
73. Regulations
74. Confidentiality
75. Transitional Provisions
76. Periodic Review
77. Savings
78. Interpretation
79. Short Title

Schedule

A LAW TO PROVIDE FOR THE RESPONSIBLE DEVELOPMENT, DEPLOYMENT, GOVERNANCE AND USE OF AUGMENTED REALITY, VIRTUAL REALITY AND SPATIAL COMPUTING TECHNOLOGIES IN AKWA IBOM STATE; TO ESTABLISH RIGHTS RELATING TO VIRTUAL SPATIAL PRIVACY AND BIOLOGICAL TELEMETRY; TO PROTECT CITIZENS AGAINST UNAUTHORISED SPATIAL TRACKING, PROFILING AND DIGITAL INTRUSION; TO PROVIDE FOR THE RESPONSIBLE CREATION AND USE OF DIGITAL TWINS OF PUBLIC INFRASTRUCTURE AND HERITAGE ASSETS; TO PROMOTE LOCAL IMMERSIVE DIGITAL CONTENT, EDUCATION, RESEARCH AND INNOVATION; AND FOR RELATED MATTERS.

BE IT ENACTED BY the Akwa Ibom State House of Assembly as follows -

{Commencement: }

PART I

Preliminary Provisions

1. The objectives are to—

(a) protect citizen's virtual spatial privacy;

(b) regulate the responsible collection and use of biological telemetry;

(c) prevent covert biometric and behavioural profiling;

(d) protect children and vulnerable persons in immersive environments;

(e) regulate the creation and commercial exploitation of digital twins of State infrastructure and heritage assets;

(f) promote responsible immersive technology;

(g) encourage local Augmented reality/Virtual reality content development;

(h) promote immersive education;

(i) support research and innovation;

(j) strengthen cybersecurity of spatial computing systems;

(k) establish appropriate remedies for unlawful spatial intrusion; and

(l) position Akwa Ibom State as a responsible centre for immersive technology development.

2. Application and Scope

(1) This Law applies, to the extent within the legislative and administrative competence of the State, to—

(a) augmented reality systems;

(b) virtual reality systems;

(c) mixed-reality systems;

(d) spatial computing platforms;

(e) immersive digital environments;

(f) spatial mapping technologies;

(g) digital twins;

(h) immersive educational platforms;

(i) virtual commerce environments;

(j) biometric and biological telemetry generated through spatial computing devices; and

(k) other immersive technologies prescribed by regulation.

(2) This Law applies to systems that are—

(a) developed;

(b) deployed;

(c) marketed;

(d) hosted;

(e) operated;

(f) procured; or

(g) used in connection with activities within Akwa Ibom State.

(3) Nothing in this Law shall be construed as—

(a) overriding the Constitution of the Federal Republic of Nigeria;

(b) replacing the Nigeria Data Protection Act or regulations made under it;

(c) restricting the lawful powers of the Nigeria Data Protection Commission;

(d) regulating matters within the exclusive legislative competence of the Federal Government; or

(e) preventing any Federal authority from exercising its lawful regulatory powers.

(4) Where a matter is subject to Federal legislation or regulation, this Law shall operate as a complementary State framework.

3. Guiding Principles

The implementation of this Law shall be guided by—

(a) privacy by design;

(b) security by design;

(c) informed consent;

(d) data minimisation;

(e) transparency;

(f) accountability;

(g) proportionality;

(h) technological neutrality;

(i) protection of children;

(j) cultural preservation;

(k) innovation; and

(l) respect for fundamental rights.

PART II

INSTITUTIONAL AND REGULATORY FRAMEWORK

4. Establishment of the Akwa Ibom State Spatial Computing and Immersive Technology Council

(1) There is established the Akwa Ibom State Spatial Computing and Immersive Technology Council, in this Law referred to as "the Council".

(2) The Governor may designate an existing State Ministry, Department or Agency to serve as the administrative host of the Council.

5. Functions of the Council

The Council shall—

(a) develop standards for immersive technology;

(b) promote virtual spatial privacy;

(c) establish technical guidance on biological telemetry;

(d) oversee State digital-twin approvals;

(e) issue compliance guidelines;

(f) investigate regulatory complaints;

(g) establish a regulatory sandbox;

(h) promote immersive education;

(i) facilitate local content development;

(j) coordinate with relevant Federal agencies;

(k) promote research and development;

(l) maintain relevant registers;

(m) conduct public awareness programmes; and

(n) perform such other functions as may be prescribed.

6. Composition of the Council

The Council shall comprise representatives of—

(a) the Ministry responsible for Science and Technology;

(b) the Ministry responsible for Culture and Tourism;

(c) the Ministry responsible for Education;

(d) the Ministry responsible for Justice;

(e) the State information and digital innovation institution;

(f) the State data-protection or privacy function, where applicable;

(g) a cybersecurity expert;

(h) an immersive-technology expert;

(i) a legal practitioner with technology-law experience; and

(j) such other persons as the Governor may appoint.

7. Appointment and Tenure

Members appointed under section 6 shall hold office for a term prescribed by the Statutory Boards Law of Akwa Ibom State, 2023.

8. Technical and Advisory Panels

The Council may establish technical panels on—

(a) biological telemetry;

(b) cybersecurity;

(c) spatial mapping;

(d) cultural heritage;

(e) education;

(f) accessibility;

(g) consumer protection; and

(h) emerging immersive technologies.

9. Meetings and Quorum

The Council shall meet at least quarterly and the quorum shall be one-half of the members of the Council.

10. Secretariat and Staff

The Council may establish a Secretariat and appoint such technical, legal, administrative and professional personnel as may be necessary.

11. Regulatory Guidelines and Standards

The Council may publish guidelines and technical standards consistent with this Law and applicable Federal legislation.

PART III

VIRTUAL SPATIAL PRIVACY AND BIOLOGICAL TELEMETRY

12. Right to Virtual Spatial Privacy

Every person has the right, subject to lawful limitations, to reasonable protection against unauthorised—

(a) tracking;

(b) behavioural monitoring;

(c) biological telemetry collection;

(d) spatial profiling;

(e) cognitive inference; and

(f) commercial exploitation within an immersive environment.

13. Definition of Biological Telemetry

For purposes of this Law, biological telemetry includes—

(a) eye-tracking logs;

(b) pupil movement;

(c) pupil dilation;

(d) gaze direction;

(e) facial micro-expressions;

(f) head movement;

(g) gait;

(h) body posture;

(i) hand and gesture movement;

(j) physiological responses;

(k) involuntary behavioural responses; and

(l) other biological or behavioural signals capable of being used to infer characteristics, preferences or reactions of an individual.

14. Classification of Spatial and Biological Data

Biological telemetry and spatial data capable of identifying or profiling an individual shall be treated as sensitive personal information for purposes of this Law and applicable data-protection legislation.

15. Consent for Collection of Biological Telemetry

(1) A person shall not collect, process or use biological telemetry for a purpose requiring consent unless the person concerned has provided—

(a) clear;

(b) informed;

(c) specific;

(d) freely given; and

(e) affirmative consent.

(2) Consent shall not be hidden within general terms of service where a separate consent is reasonably required.

16. Prohibition of Covert Telemetry Collection

A person shall not knowingly deploy an immersive system designed to secretly collect biological telemetry without lawful authority or valid consent.

17. Purpose Limitation and Data Minimisation

An operator shall collect only biological or spatial data reasonably necessary for the declared purpose of the service.

18. Prohibition of Unauthorised Sale or Trading of Telemetry

A person shall not sell, trade, rent or otherwise commercially transfer biological telemetry for a purpose materially different from the purpose for which it was lawfully collected without an appropriate legal basis and, where required, consent.

19. Retention and Deletion of Telemetry

Biological telemetry shall not be retained longer than reasonably necessary for the lawful purpose for which it was collected.

20. Right of Access, Correction and Withdrawal

A user shall, subject to applicable law, have the right to—

(a) know whether biological telemetry is being processed;

(b) access relevant information;

(c) request correction of inaccurate information;

(d) withdraw consent where consent is the applicable legal basis; and

(e) request deletion where legally applicable.

21. Profiling and Behavioural Inference

A person shall not use biological telemetry to infer sensitive personal characteristics or psychological states in a manner that is unlawful, discriminatory, deceptive or materially harmful.

22. Children's Virtual Spatial Privacy

Operators providing immersive services reasonably likely to be accessed by children shall implement enhanced safeguards against—

(a) covert tracking;

(b) behavioural profiling;

(c) targeted exploitation;

(d) inappropriate advertising;

(e) manipulation; and

(f) unauthorised collection of biological telemetry.

PART IV

IMMERSIVE SYSTEMS SAFETY AND CONSUMER PROTECTION

23. Transparency Requirements

An immersive service shall clearly disclose—

(a) the identity of the operator;

(b) the categories of data collected;

(c) the purpose of collection;

(d) whether biological telemetry is collected;

(e) whether data is shared with third parties;

(f) retention periods where applicable; and

(g) available privacy controls.

24. Safety-by-Design

Providers shall, so far as reasonably practicable, incorporate safety and privacy safeguards into immersive systems from the design stage.

25. Immersive Content Disclosures

Where an immersive experience contains simulated environments, artificial characters or materially altered representations of real persons or places, the provider shall provide appropriate disclosure where failure to do so could materially mislead users.

26. Manipulative or Deceptive Immersive Experiences

A provider shall not intentionally design an immersive environment to exploit a user's vulnerability in a manner that causes material harm.

27. Spatial Harassment and Digital Intrusion

A person shall not intentionally use an immersive environment to—

(a) stalk;

(b) threaten;

(c) sexually harass;

(d) intimidate;

(e) impersonate; or

(f) unlawfully intrude upon another person's protected virtual or spatial environment.

28. Protection Against Unauthorised Recording

A person shall not intentionally record or capture another person's private immersive interaction where the recording is unlawful or contrary to applicable privacy law.

29. Accessibility and Inclusion

Providers of public immersive services shall, where reasonably practicable, design systems accessible to persons with disabilities.

30. Consumer Complaints and Redress

The Council shall establish a mechanism through which users may lodge complaints concerning—

(a) unlawful telemetry collection;

(b) privacy violations;

(c) deceptive immersive services;

(d) unauthorised profiling;

(e) digital-twin misuse; and

(f) other breaches of this Law.

31. Platform Accountability

A provider shall maintain reasonable procedures for responding to valid complaints and material privacy or security incidents.

PART V

DIGITAL TWINS, SPATIAL MAPPING AND STATE HERITAGE

32. Regulation of Public Digital Twins

A person or corporate entity seeking to create a detailed commercial digital twin of—

(a) State-owned infrastructure;

(b) major public buildings;

(c) designated State facilities;

(d) public monuments;

(e) protected heritage sites; or

(f) designated cultural assets

shall comply with applicable approval requirements.

33. Digital Twin Clearance

The Council, in consultation with the Ministry responsible for Culture and Tourism and any relevant State institution, shall establish a Digital Twin Clearance System which shall address—

(a) cultural integrity;

(b) security;

(c) intellectual-property considerations;

(d) privacy;

(e) commercial exploitation;

(f) attribution; and

(g) public-interest considerations.

34. Mapping of State Infrastructure

Where a proposed spatial scan could expose sensitive information concerning critical infrastructure, additional security safeguards may be required.

35. Digital Replication of Heritage Assets

A person shall not commercially reproduce, modify or exploit a designated State heritage asset through a digital twin in a manner prohibited by applicable law or without required State clearance.

36. Cultural and Heritage Data Register

The Ministry responsible for Culture and Tourism may establish a register of designated heritage assets requiring special protection against unauthorised digital replication.

37. Commercial Exploitation of State Digital Twins

A person commercially exploiting an approved digital twin of a designated State heritage asset may be required to—

(a) identify the origin of the asset;

(b) comply with prescribed licensing terms;

(c) provide appropriate attribution; and

(d) contribute to applicable cultural-preservation programmes.

38. Attribution and Benefit-Sharing

Regulations may provide for reasonable benefit-sharing arrangements for commercial exploitation of designated State heritage digital assets, subject to applicable intellectual-property and public-finance laws.

39. Exceptions for Education, Research and Public Interest

The Council shall exempt bona fide—

(a) educational;

(b) academic;

(c) research;

(d) museum;

(e) preservation; and

(f) public-interest projects from specified clearance fees or requirements.

40. Security of Critical Spatial Models

A person shall not knowingly publish or distribute a detailed spatial model of designated critical infrastructure where the publication creates a material security risk and is prohibited by applicable law.

PART VI

DATA GOVERNANCE, CYBERSECURITY AND SPATIAL SECURITY

41. Spatial Data Governance

Operators shall establish appropriate controls for—

(a) collection;

(b) storage;

(c) access;

(d) processing;

(e) sharing; and

(f) deletion of spatial data.

42. Cybersecurity Requirements

Immersive technology providers shall implement reasonable cybersecurity measures proportionate to the risk of their systems.

43. Protection Against Spatial System Hijacking

A person shall not unlawfully access, manipulate or take control of an immersive or spatial computing system.

44. Encryption and Access Controls

Sensitive spatial and biological telemetry shall be protected through appropriate technical and organisational safeguards.

45. Incident Reporting

A provider shall report a material security breach involving sensitive spatial or biological telemetry to the appropriate authority within the period prescribed by applicable law.

46. Data Storage and Cross-Border Transfers

Nothing in this Law shall impose an absolute prohibition on lawful cross-border processing. However, operators processing sensitive spatial or biological telemetry shall comply with applicable Nigerian data-protection requirements and prescribed safeguards.

47. Audit Trails and Technical Records

Regulated providers shall maintain appropriate technical records sufficient to establish—

(a) what categories of data were collected;

(b) the purpose;

(c) access;

(d) material disclosures;

(e) security incidents; and

(f) deletion or retention where applicable.

PART VII

EDUCATION, INNOVATION AND LOCAL CONTENT

48. Immersive Technology Regulatory Sandbox

The Council shall establish an **Akwa Ibom Immersive Technology Regulatory Sandbox** for controlled development and testing of innovative AR, VR and spatial computing technologies.

49. Eligibility for Sandbox Participation

An applicant shall demonstrate—

(a) technological innovation;

(b) a defined public or commercial benefit;

(c) a privacy and data-governance plan;

(d) cybersecurity safeguards;

(e) risk assessment;

(f) user-protection measures; and

(g) appropriate human oversight.

(h) priority may be given to projects addressing—

i. education;
ii. healthcare;
iii. agriculture;
iv. tourism;
v. culture;

vi. manufacturing;

vii. public services; and

viii. accessibility.

50. Sandbox Safeguards and Testing Limits

Sandbox participants shall—

(a) disclose that the service is undergoing regulatory testing;

(b) restrict testing to approved users and environments;

(c) maintain appropriate data controls;

(d) provide emergency suspension mechanisms;

(e) comply with privacy safeguards; and

(f) maintain appropriate technical records.

51. Exit Pathways and Certification

At the conclusion of the sandbox, the Council shall—

(a) grant compliance certification;

(b) grant a conditional extension; or

(c) require the system to cease testing or deployment within the State.

This mirrors the three-pathway exit model already developed for the AI Sandbox.

52. Educational AR/VR Content Development

The Government shall encourage the development of immersive educational content aligned with the approved curriculum of Akwa Ibom schools and priority areas may include—

(a) science;

(b) mathematics;

(c) technology;

(d) history;

(e) geography;

(f) culture;

(g) agriculture;

(h) vocational education; and

(i) technical skills.

53. Local Immersive Content Incentives

(1) Subject to applicable tax laws and the lawful taxing powers of the State, the Government may provide incentives for eligible local enterprises developing approved educational AR/VR content. Such incentives may include—

(a) grants;

(b) innovation funding;

(c) procurement preference;

(d) fee waivers;

(e) sandbox fee exemptions;

(f) State-level tax or levy incentives within lawful competence; and

(g) recommendations to relevant tax authorities for applicable Federal incentives.

(2) The Government may, subject to applicable Federal and State tax laws, provide or facilitate incentives equivalent to or up to 35% of qualifying State-administered taxes, levies, fees or approved innovation expenditure.

54. Research and Development Exemptions

Academic and bona fide research projects shall receive exemptions from specified registration or processing fees as determined by the Council.

55. Skills Development and Local Capacity

The Government shall promote—

(a) Augmented reality/Virtual reality development;

(b) 3D modelling;

(c) spatial computing;

(d) immersive design;

(e) digital heritage preservation;

(f) cybersecurity;

(g) digital arts; and

(h) technical certification.

56. Public-Private Partnerships

The Government may enter into partnerships with—

(a) universities;

(b) technology companies;

(c) museums;

(d) cultural institutions;

(e) schools;

(f) tourism operators; and

(g) investors

for immersive technology development.

PART VIII

OFFENCES, PENALTIES AND REMEDIES

57. Unlawful Collection of Biological Telemetry

(a) a person who knowingly collects biological telemetry without the required legal basis commits an offence.

Individual: up to ₦5,000,000 fine

Corporate entity: up to ₦20,000,000 fine

(b) where the violation affects more than 1,000 individuals, the corporate penalty may be increased to ₦50,000,000.

58. Unauthorised Sale or Disclosure of Telemetry

A person who knowingly sells, trades or unlawfully discloses protected biological telemetry commits an offence.

Individual: up to ₦10,000,000 fine or confinement up to three years, or both.

Corporate entity: up to ₦30,000,000 fine

59. Unlawful Spatial Tracking and Profiling

A person who knowingly uses immersive technology to conduct unlawful tracking or profiling commits an offence.

Individual: up to ₦5,000,000 fine.

Corporate entity: up to ₦25,000,000 fine.

60. Spatial Harassment and Digital Intrusion

A person who intentionally uses an immersive environment to stalk, threaten, harass or unlawfully intrude upon another person commits an offence.

The Court may impose—

(a) a fine;

(b) compensation;

(c) an injunction;

(d) an order requiring removal of offending content; or

(e) any other remedy available under applicable law.

61. Unauthorised Digital Twin Replication

(a) a person who knowingly creates and commercially exploits a protected State digital twin without required clearance commits an offence.

Individual: up to ₦5,000,000 fine.

Corporate entity: up to ₦20,000,000 fine.

(b) where the activity materially compromises critical infrastructure security, the penalty may be increased to ₦50,000,000.

62. Fraudulent or Deceptive Immersive Services

A person who intentionally uses immersive technology to defraud, impersonate or materially deceive another person commits an offence.

Individual: up to ₦10,000,000 fine or confinement up to five years, or both.

Corporate entity: up to ₦30,000,000 fine.

63. Cybersecurity Violations

A person who knowingly—

(a) hijacks;

(b) compromises;

(c) disables;

(d) manipulates; or

(e) unlawfully accesses a regulated spatial computing system commits an offence.

Individual: up to ₦15,000,000 or confinement up to five years, or both.

Corporate entity: up to ₦50,000,000.

64. Corporate Liability

Where an offence is committed by a corporate body with the consent, connivance or neglect of a director, manager or responsible officer, the relevant person may be liable in accordance with extant criminal Law.

65. Continuing Offences

Where a person continues to breach a compliance order after receiving notice, an additional administrative penalty of up to ₦500,000 per day may be imposed.

66. Administrative Sanctions

The Council may impose proportionate administrative measures including—

(a) warning;

(b) compliance notice;

(c) corrective action;

(d) suspension;

(e) withdrawal of State certification;

(f) administrative monetary penalty;

(g) exclusion from the regulatory sandbox;

(h) suspension from State procurement; and

(i) referral to a competent Federal authority.

67. Compensation and Civil Remedies

A person whose rights under this Law have been violated may seek appropriate remedies, including—

(a) compensation;

(b) injunction;

(c) deletion of unlawfully collected data;

(d) cessation of unlawful processing;

(e) restoration of privacy; and

(f) other remedies available under applicable law.

68. Appeals and Judicial Review

A person affected by a decision of the Council may appeal in accordance with regulations and may seek judicial review before a competent court.

PART IX

FINANCE, FEES AND MISCELLANEOUS

69. Fees and Charges

(1)The Council shall prescribe reasonable fees for—

(a) regulatory registration;

(b) digital-twin clearance;

(c) technical assessment;

(d) compliance certification;

(e) inspection;

(f) sandbox participation;

(g) specialist assessment; and

(h) other regulatory services.

(2) Initial Fee Framework:

Service	**Proposed Maximum Fee**
Academic/research registration	**Nil**
Basic immersive technology registration	**₦100,000**
Commercial AR/VR operator registration	**₦250,000**
High-risk spatial computing assessment	**₦500,000**
Digital Twin Clearance – ordinary	**₦250,000**
Digital Twin Clearance – major commercial project	**₦500,000–₦1,000,000**
Technical/privacy assessment	**₦250,000–₦750,000**
Annual renewal	**50% of initial fee**
University sandbox	**Nil**
Early-stage/start-up sandbox	**Nil**
Large commercial sandbox	**Cost recovery**

70. Funding of the Council

The Council shall be funded through—

(a) appropriations by the House of Assembly;

(b) prescribed fees;

(c) lawful grants;

(d) donations;

(e) development partnerships; and

(f) other lawful sources.

71. Accounts and Audit

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

72. Annual Report

The Council shall submit an annual report to the Governor and House of Assembly covering—

(a) registrations;

(b) privacy complaints;

(c) enforcement;

(d) digital-twin approvals;

(e) sandbox activities;

(f) innovation programmes;

(g) educational projects;

(h) finances; and

(i) recommendations.

73. Regulations

The Council may, subject to required approval, make regulations concerning—

(a) biological telemetry;

(b) spatial privacy;

(c) digital twins;

(d) data protection;

(e) cybersecurity;

(f) risk classification;

(g) immersive content;

(h) sandbox administration;

(i) fees;

(j) enforcement;

(k) educational incentives; and

(l) other matters necessary to give effect to this Law.

74. Confidentiality

Members, officers, consultants and persons acting under this Law shall maintain the confidentiality of information obtained in the performance of their duties except where disclosure is authorised or required by law.

75. Transitional Provisions

A person lawfully operating an immersive technology service at commencement shall have twelve months to comply with this Law, unless the Council determines that immediate action is required to prevent serious harm.

76. Periodic Review

The Council shall review this Law not later than three years after commencement and every three years thereafter, taking into account—

(a) technological developments;

(b) Federal regulatory developments;

(c) privacy risks;

(d) economic impact;

(e) innovation;

(f) cultural preservation; and

(g) enforcement experience.

77. 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.

78. Interpretation

In this law-

“augmented reality” means technology that overlays digitally generated content onto a user’s perception of the physical environment;

“biological telemetry” means data generated from the physical, physiological, behavioural or involuntary responses of a person through an immersive or spatial computing system;

“digital twin” means a digital representation of a physical object, person, building, infrastructure, location or environment that is capable of being used for analysis, simulation, visualisation or interaction;

“immersive environment” means a digital or digitally enhanced environment designed to create a perception or presence or interaction.

“provider” means any person or entity that develops, supplies, operates, deploys or make available an augmented reality, virtual reality or spatial computing system, service or application;

“spatial computing” means computing technologies that understand, map, represent or interact with physical space or objects;

“spatial data” means data relating to the location, geometry, movement or physical characteristics of persons, objects, buildings or environment;

“virtual spatial privacy” means the right of an individual to reasonable protection against unauthorised collection, inference, tracking or exploitation of personal spatial, behavioural or biological information within immersive environments;

“virtual reality” means technology that creates a digitally simulated environment capable of immersive interaction

79. Short Title

This Law may be cited as the Akwa Ibom State Augmented Reality, Virtual Reality, and Spatial Computing Protection Law, 2026.

SCHEDULES

SCHEDULE 1

RISK-BASED CLASSIFICATION OF IMMERSIVE SYSTEMS

The Council may classify immersive systems according to their potential impact on privacy, safety, security and fundamental rights.

1. PROHIBITED OR UNLAWFUL USES

Examples include:

(a) covert biological telemetry collection;

(b) unlawful mass spatial surveillance;

(c) immersive systems deliberately designed to manipulate vulnerable persons causing material harm;

(d) unlawful biometric profiling;

(e) malicious spatial intrusion;

(f) systems designed to facilitate serious criminal activity.

2. HIGH-RISK SYSTEMS

Examples include systems used for—

(a) healthcare;

(b) employment;

(c) education assessment;

(d) critical infrastructure;

(e) public safety;

(f) sensitive biometric analysis;

(g) highly consequential behavioural profiling.

These should require enhanced privacy, cybersecurity, testing and human oversight.

3. LIMITED-RISK SYSTEMS

Examples include—

(a) commercial entertainment;

(b) virtual shopping;

(c) advertising;

(d) ordinary gaming;

(e) tourism experiences.

These should primarily be subject to transparency and consumer-protection requirements.

4. MINIMAL-RISK SYSTEMS

Examples include—

(a) ordinary educational visualisation;

(b) artistic experimentation;

(c) non-sensitive gaming;

(d) basic 3D visualisation.

These should receive proportionate oversight.

SCHEDULE 2

MINIMUM VIRTUAL SPATIAL PRIVACY REQUIREMENTS

A regulated immersive platform should, where applicable, provide:

1. Clear privacy notice.
2. Separate consent for sensitive telemetry.
3. Ability to withdraw consent.
4. Data minimisation.
5. Encryption.
6. Access controls.
7. Data deletion mechanisms.
8. User-access mechanisms.
9. Protection against covert tracking.
10. Children's privacy safeguards.
11. Security incident procedures.
12. Appropriate retention controls.
13. Audit logs.
14. Human support and complaint mechanisms.

SCHEDULE 3

DIGITAL TWIN CLEARANCE CATEGORIES

Category A — Low Sensitivity

Examples:

i. public tourism sites;
ii. educational models;
iii. general cultural visualisations.

Requirement: notification or simplified clearance.

Category B — Protected Cultural Assets

Examples:

i. museums;
ii. monuments;
iii. designated heritage buildings;
iv. culturally significant locations.

Requirement: cultural clearance and attribution.

Category C — Sensitive Public Infrastructure

Examples:

i. electricity infrastructure;
ii. telecommunications facilities;
iii. water infrastructure;
iv. security-sensitive facilities.

Requirement: enhanced technical and security assessment.

THE FIVE CORE POLICY PILLARS

Pillar	**Policy objective**
Virtual Spatial Privacy	Protect citizens' immersive behavioural and biological data
Biological Telemetry Firewall	Prevent covert collection and unauthorised trading
Digital Twin Sovereignty	Protect designated State heritage and sensitive public assets
Immersive Education	Build AR/VR content around the State curriculum

Pillar	Policy objective
Innovation Sandbox	Allow companies to develop and test safely