



Tuvalu

ONLINE GAMING REGULATION

2023 REVISED EDITION

CAP 50.03



Tuvalu

ONLINE GAMING REGULATION

Arrangement Of Sections

Section	Page
1. Short Title	6
2. Establishment of Framework	6
3. Purpose	6
4. Scope	7
5. Prohibition	7
6. Interpretation.....	7

PRAT II - LICENSING AND OPERATIONAL REQUIREMENTS

7. Authorization	8
8. Scope	8
9. Prevention of Unauthorized Access	8
10. Certification of Gaming Systems	8
11. Data Centers and Security	9
12. API Connections	9
13. White Label Operators	9
14. Domain Management	9
15. Application Submission	9
16. Due Diligence	8
17. Commitment to Compliance	8
18. Domain Ownership	9
19. License Validity	9
20. Renewal Applications	10
21. License Fees	10
22. Non-Compliance	10
23. Currency and Source of Funds	10

PART III - REGULATORY OVERSIGHT AND REPORTING OBLIGATIONS

24. Regulatory Body	10
25. Authorized Representative	10
26. Public Register	10
27. Continuous Monitoring	10

28. Inspections and Audits	10
29. Communication Channels	11
30. Complaint Handling	11
31. Immediate Notification	11
32. Annual Submissions	11
33. Access to Data	11
34. Third-Party Providers	11
35. AI Usage	11

PART IV - PLAYER PROTECTION, RESPONSIBLE GAMING, AND AML MEASURES

36. Advanced Tools	11
37. Verification and Due Diligence	11
38. Monitoring and Intervention	12
39. Dormant Accounts	12
40. Bonus Offers	12
41. Transparency of Odds	12
42. Player Controls	12
43. Complaint Policy	12
44. AML/CFT Programs	12
45. High-Risk Customers	12
46. Record Keeping	12
47. Reporting Suspicious Activities	13
48. Chargebacks and Fraud	13
49. Virtual Asset Policy	13
50. Compliance Officer	13
51. Third-Party Fraud	13

PART V - TAXATION AND FINANCIAL CONTRIBUTIONS

52. Gaming Tax	13
53. Annual Fees	13

PART VI - ADVERTISING, MARKETING, AND BRANDING RESTRICTIONS

54. Legal Jurisdictions	13
55. Targeting Restrictions	13
56. Responsible Gaming Messages	14
57. Storage of Materials	14

PART VII - ENFORCEMENT, PENALTIES, AND DISPUTE RESOLUTION

58. Legal Jurisdictions	14
59. Targeting Restrictions	14
60. Responsible Gaming Messages	14
61. Storage of Materials	14
62. Affiliate Approval	14
63. Language Approval	14
64. License Display	14

PART VIII – CYBERSECURITY

65. Targeting Tuvaluan Citizens	15
66. Operating in Restricted Jurisdictions	15
67. Non-Compliance	15
68. Authority Powers	15
69. Public Warnings	15
70. Asset Seizure	15
71. Account Closure	15

PART IX – DATA PROTECTION

72. Multi-Factor Authentication	15
73. Data Encryption	16
74. Data Breach Response	16

PART X – AI USAGE

75. Data Protection Standards	16
76. Data Protection Policy	16
77. Data Breach Notification	16
78. Data Transfer Policy	16
79. Player Access to Data	16

PART XI - DORMANT ACCOUNTS AND UNCLAIMED WINNINGS

80. AI Usage Disclosure	16
81. Independent AI Audits	16
82. AI Transparency	17
83. Regular AI Updates	17

PART XII – MISCELLANEOUS

84. Dormant Account Policy	17
85. Unclaimed Winnings Procedure	17
86. Transfer to Authority	17

PART XIII - Final Provisions

87. Severability	17
88. Commencement and Enactment	17
89. Prior license	17
90. Application submission starting date	17
91. Regulation development	17



Tuvalu

ONLINE GAMING REGULATION

AN ACT to regulate online gaming operations under the jurisdiction of Tuvalu, ensuring compliance with international best practices and protecting the integrity of the industry.

1. Short Title

This Act shall be cited as the Tuvalu Gaming Authority Online Gaming License Act, 2024.

2. Establishment of Framework

This Act establishes a legal and regulatory framework for the licensing, supervision, auditing, and enforcement of Online Gaming Licenses issued under the jurisdiction of Tuvalu for operators providing services exclusively outside of Tuvalu.

3. Purposes

The purposes of this Act are to:

- (1) Maintain a world-leading regulatory regime aligned with international standards, best practices, and technological advancements.
- (2) Ensure online gaming services are categorically inaccessible to Tuvaluan citizens and residents, regardless of any circumvention methods.
- (3) Proactively prevent gambling-related harm through advanced responsible gaming measures, player protection, and early intervention protocols.
- (4) Aggressively combat money laundering, terrorist financing, and other financial crimes.
- (5) Ensure fair gaming practices, regulatory integrity, and public trust through rigorous oversight and transparency.
- (6) Protect player funds and data with the highest level of security and privacy.
- (7) Promote technological security, ethical conduct, and responsible advertising practices.
- (8) Create a controlled “sandbox” environment for the testing and development of innovative gaming technologies.
- (9) Establish a clear procedure for dealing with dormant accounts, unclaimed winnings, and player disputes.

4. Scope

This Act applies to all entities involved in online gaming operations under Tuvalu's jurisdiction, including but not limited to operators and software providers.

5. Prohibition

Online gaming within the territorial boundaries of Tuvalu is strictly prohibited.

6. Interpretation

In this Act, unless the context otherwise requires —

"Authorized Representative" - means a private company or individual appointed by the Authority to act as its official representative in all related to the license, including onboarding, communication, process management functions, collecting any fees and financial liabilities, subject to the terms and conditions set forth in a written agreement with the Authority.

"Behavioral Analysis" - The use of data analysis to identify patterns of player behavior.

"Data Breach Incident Response Plan": A detailed plan for responding to data security breaches.

"Enhanced Due Diligence (EDD)" - Additional measures to verify the identity and source of funds for high-risk customers.

"External Security Audit" - An independent assessment of an operator's security infrastructure.

"Fraud Detection System" - Technology used to identify and prevent fraudulent activities.

"High-Risk Transaction" - A transaction that exceeds a specified monetary threshold or exhibits suspicious patterns.

"Internal Control System" - Policies and procedures to ensure compliance with regulatory requirements.

"Live Dealer Studio Inspection": An on-site inspection of a live dealer studio to ensure fairness and security.

"Multi-Factor Authentication (MFA)" - A security measure that requires multiple forms of verification.

"Network Security Assessment" - An evaluation of the security of an operator's network infrastructure.

"Payment Gateway Security Audit" - An audit of the security of a payment gateway.

"Restricted Jurisdictions" - Afghanistan, China, Cuba, Central African Republic, Democratic Republic of Congo, Haiti, Iran, Iraq, Israel, Libya, Myanmar, North Korea, Russia, Somalia, South Sudan, Syria, UK, USA, Yemen, Venezuela, any jurisdiction added to the black list by the FATF and any jurisdiction with restriction on non-local license holders.

"Risk-Based Approach" - A regulatory approach that focuses on identifying and mitigating high-risk activities.

"Software Vulnerability Scanning" - The process of identifying security vulnerabilities in gaming software.

"Third-Party Certification" - Certification from an independent organization that an operator meets specific standards.

"Unclaimed Winnings" - Winnings that have not been claimed by a player within a

specified period.

"Virtual Asset Transaction Monitoring" - The monitoring of transactions involving virtual assets for suspicious activity.

"Source Code Analysis" - an independent review of gaming software.

"IP Geofencing" - The use of technology to prevent access from restricted IP addresses.

"Dynamic KYC" - Ongoing KYC checks based on player behaviour.

"Affiliate Marketing" - Marketing activities conducted by third parties to promote online gaming services.

"Dormant Account" - A player account that has been inactive for a specified period.

"Escrow Account" - A secure account held by a third party for player funds.

"Geolocation Verification" - Technology used to confirm a player's location.

"High-Risk Customer" - A customer identified as posing a higher risk of money laundering or terrorist financing.

"Live Dealer Studio" - A facility where live dealer games are conducted.

"Material Change" - Any significant change in an operator's ownership, control, or operations.

"Payment Gateway" - A service that authorizes credit card or direct payment processing.

"Software Audit Trail" - A record of all changes made to gaming software.

"Virtual Assets" - Digital representations of value that can be digitally traded or transferred.

"White Label Operator" - An operator that uses another company's gaming platform.

"API" - Application Programming Interface.

PART II - LICENSING AND OPERATIONAL REQUIREMENTS

7. Authorization

The Tuvalu Gaming Authority is exclusively authorized to issue Online Gaming Licenses to operators who meet the most stringent criteria.

8. Scope

Licenses shall specify the types of gaming activities, software providers, payment processors, and third-party service providers authorized for use, with mandatory restrictions on any activity that poses a heightened risk of harm or illegality.

9. Prevention of Unauthorized Access

Operators must implement robust IP geofencing, geolocation verification, and other measures to prevent access from Restricted Countries and High-Risk Jurisdictions, with regular audits of these systems.

10. Certification of Gaming Systems

All gaming systems, including RNGs, live dealer studios, and AI-driven algorithms, must be certified by independent testing laboratories, with source code analysis and software vulnerability scanning.

11. Data Centers and Security

Operators must maintain redundant and geographically diverse data centers, with mandatory disaster recovery testing, failover procedures, and external security audits.

12. API Connections

Operators must have a clear policy on the use of API connections to third parties, with security audits of all connected systems.

13. White Label Operators

Operators must provide a full list of all White Label operators that they work with, and ensure those operators comply with all Tuvalu regulations.

14. Domain Management

Operators must provide a full list of all domains that they intend to operate and must receive approval from the authority approval for any domain.

15. Application Submission

Applicants must submit detailed business plans, financial statements, compliance documentation, risk assessments, and internal control systems.

16. Due Diligence

Due diligence shall include background checks, financial audits, technical assessments, and analysis of shareholder directors and key persons of the applicant.

17. Commitment to Compliance

Applicants must demonstrate an unwavering commitment to responsible gaming, AML/CFT compliance, data protection, cybersecurity, and ethical conduct, with mandatory third-party certifications.

18. Domain Ownership

Applicants must provide a full list of all domains that they intend to operate, and provide documentation of the ownership of those domains.

19. License Validity

Online Gaming Licenses shall be issued for a limited period, not exceeding one year, and may be renewed subject to rigorous review and approval by the Authority.

20. Renewal Applications

Renewal applications must be submitted at least 30 days before the expiration of the license, accompanied by updated documentation, audit reports, compliance certifications, and evidence of continuous improvement.

21. License Fees

License fees shall be paid to the Authority, with mandatory fee schedules and payment deadlines.

22. Non-Compliance

Failure to comply with renewal requirements or any provision of this Act shall result in automatic license suspension or revocation, and the imposition of severe financial penalties, including forfeiture of assets.

23. Currency and Source of Funds

All fees will be paid in a currency set by the authority, and operators must provide proof of the source of those funds.

PART III - REGULATORY OVERSIGHT AND REPORTING OBLIGATIONS

24. Regulatory Body

The Tuvalu Gaming Authority shall be the regulatory body responsible for the licensing, supervision, enforcement, and auditing of Online Gaming Licenses, with full autonomy and independence if not indicated otherwise in this act.

25. Authorized Representative

The Authority may, by written agreement, appoint an Authorized Representative to perform specific onboarding, communication, and process management functions, subject to strict confidentiality, data protection, and performance standards as prescribed by the Authority.

26. Public Register

The Authority shall maintain a public register of all licensed operators.

27. Continuous Monitoring

The Authority shall conduct continuous real-time monitoring of gaming activities, transactions, and player behavior.

28. Inspections and Audits

The Authority shall conduct inspections, forensic audits, cybersecurity assessments, and live dealer studio inspections of licensed operators.

29. Communication Channels

The Authority shall establish and maintain secure communication channels for reporting suspicious activities, compliance violations, and player complaints, with whistleblower protection and anonymity.

30. Complaint Handling

The authority will create a system for reporting and tracking player complaints, with mandatory response times for operators.

31. Immediate Notification

Operators shall immediately notify the Authority of any material changes, suspicious activities, compliance violations, data breaches, and cybersecurity incidents, with detailed incident reports and remediation plans.

32. Annual Submissions

Operators shall submit annual audited financial statements, cybersecurity reports, responsible gaming reports, AML/CFT compliance reports, and external security audit reports to the Authority, with mandatory third-party certifications.

33. Access to Data

Operators must provide immediate and unrestricted access to all data, records, systems, and personnel to the Authority upon request, with mandatory data retention policies and audit trails.

34. Third-Party Providers

Operators must report any changes to third-party technology providers, including detailed information on their services, compliance status, and security measures, and provide a comprehensive list of all third-party providers.

35. AI Usage

Operators must report all use of AI, including detailed explanations of the AI systems, its algorithms, and its use cases.

PART IV - PLAYER PROTECTION, RESPONSIBLE GAMING, AND AML MEASURES

36. Advanced Tools

Operators shall implement responsible gaming tools and policies.

37. Verification and Due Diligence

Operators shall conduct mandatory age verification, KYC checks, and EDD for high-risk players, with dynamic KYC checks based on player behavior and transaction patterns.

38. Monitoring and Intervention

Operators shall monitor player behavior for signs of excessive spending, frequent deposits, and unusual playing patterns, and implement proactive intervention measures, with mandatory behavioral analysis and risk profiling.

39. Dormant Accounts

Operators shall have a clear and transparent dormant account policy, with mandatory notification and return of unclaimed winnings.

40. Bonus Offers

Operators shall have a clear and transparent policy on the use of bonus offers and promotions, with mandatory terms and conditions and responsible marketing practices.

41. Transparency of Odds

Operators shall provide full transparency of all game odds, RTP (return to player) percentages, and payout tables, with mandatory independent testing and certification.

42. Player Controls

Operators must provide a “cooling off” period and a way to set session time limits.

43. Complaint Policy

Operators must have a policy for dealing with player complaints.

44. AML/CFT Programs

Operators shall implement robust AML/CFT programs, including transaction monitoring, customer due diligence, EDD, and suspicious activity reporting, with transaction monitoring and risk scoring.

45. High-Risk Customers

Operators shall conduct enhanced due diligence for high-risk customers, high-risk transactions, and politically exposed persons (PEPs), with mandatory source of funds verification and beneficial ownership disclosure.

46. Record Keeping

Operators shall maintain detailed records of all transactions, player accounts, compliance activities, and AML/CFT investigations, with mandatory data retention policies and audit trails.

47. Reporting Suspicious Activities

Operators shall report all suspicious activities to the Authority and relevant law enforcement agencies, including the Financial Intelligence Unit (FIU), with mandatory reporting templates and secure communication channels.

48. Chargebacks and Fraud

Operators must have a comprehensive process for dealing with chargebacks, fraud investigations, and dispute resolutions, with mandatory fraud detection systems and prevention measures.

49. Virtual Asset Policy

Operators must have a clear and transparent policy on the use of virtual assets, including transaction monitoring, risk assessments, and compliance measures.

50. Compliance Officer

Operators must have a designated AML/CFT compliance officer, with mandatory training and certification.

51. Third-Party Fraud

Operators must have a system for dealing with fraud related to 3rd party providers.

PART V - TAXATION AND FINANCIAL CONTRIBUTIONS**52. Gaming Tax**

Online Gaming License holders shall not be subject to a gaming tax.

53. Annual Fees

Operators shall pay annual fees to the Authority, with mandatory fee schedules and payment deadlines.

PART VI - ADVERTISING, MARKETING, AND BRANDING RESTRICTIONS**54. Legal Jurisdictions**

License holders may only advertise their services in jurisdictions where online gaming is legally permitted.

55. Targeting Restrictions

Advertising must not target minors, vulnerable persons, or residents of Restricted Countries and High-Risk Jurisdictions, with mandatory age verification and geolocation restrictions.

56. Responsible Gaming Messages

Operators shall include prominent and visible responsible gaming messages, age restrictions, and helpline information in all advertisements, with mandatory compliance with advertising standards and codes of conduct.

57. Storage of Materials

All marketing materials, including affiliate marketing activities, shall be stored for auditing purposes, with mandatory data retention policies and audit trails.

PART VII - ENFORCEMENT, PENALTIES, AND DISPUTE RESOLUTION

58. Legal Jurisdictions

License holders may only advertise their services in jurisdictions where online gaming is legally permitted.

59. Targeting Restrictions

Advertising must not target minors, vulnerable persons, or residents of Restricted Countries and High-Risk Jurisdictions, with mandatory age verification and geolocation restrictions.

60. Responsible Gaming Messages

Operators shall include prominent and visible responsible gaming messages, age restrictions, and helpline information in all advertisements, with mandatory compliance with advertising standards and codes of conduct.

61. Storage of Materials

All marketing materials, including affiliate marketing activities, shall be stored for auditing purposes, with mandatory data retention policies and audit trails.

62. Affiliate Approval

All affiliate marketing activities must be approved by the Authority, with mandatory affiliate agreements and compliance monitoring.

63. Language Approval

All advertising must be in languages approved by the Authority, with mandatory translation services and language proficiency.

64. License Display

All advertising must clearly and prominently display the operator's license information, with mandatory license verification and display requirements.

PART VII - ENFORCEMENT, PENALTIES, AND DISPUTE RESOLUTION**65. Targeting Tuvaluan Citizens**

Engaging in online gaming operations targeting Tuvaluan citizens shall result in immediate and permanent revocation of the license, criminal prosecution, and mandatory asset forfeiture and public disclosure.

66. Operating in Restricted Jurisdictions

Providing gaming services in Restricted Countries and High-Risk Jurisdictions shall be punishable by crippling fines, permanent disqualification from the Tuvalu licensing system, and public disclosure, with mandatory blacklisting and asset seizure.

67. Non-Compliance

License holders failing to comply with reporting, auditing, compliance, or cybersecurity requirements shall face severe penalties, including financial sanctions, license suspension, criminal prosecution, and public disclosure, with mandatory remedial actions and compliance plans.

68. Authority Powers

The Authority can issue fines, suspend, or revoke licenses, with mandatory penalty schedules and enforcement procedures.

69. Public Warnings

The Authority can issue public warnings, compliance orders, and cease and desist orders, with mandatory publication and enforcement mechanisms.

70. Asset Seizure

The Authority shall have the power to freeze player funds, seize assets, and initiate legal proceedings, with mandatory legal representation and due process.

71. Account Closure

The authority will have the power to force operators to close player accounts.

PART VIII – CYBERSECURITY**72. Multi-Factor Authentication**

Operators must use multi-factor authentication (MFA) for all staff accounts, with mandatory access controls and security protocols.

73. Data Encryption

Operators must encrypt all customer data, with mandatory data encryption standards and key management systems.

74. Data Breach Response

Operators must have a detailed data breach incident response plan, with mandatory notification procedures and remediation measures.

PART IX – DATA PROTECTION

75. Data Protection Standards

Operators must adhere to the Authority's comprehensive data protection standards, with mandatory compliance with international data protection laws and regulations.

76. Data Protection Policy

Operators must have a comprehensive data protection policy, with mandatory provisions for data collection, processing, storage, and transfer.

77. Data Breach Notification

Operators must have a data breach notification policy, with mandatory notification procedures and timelines.

78. Data Transfer Policy

Operators must have a data transfer policy, with mandatory safeguards for international data transfers.

79. Player Access to Data

Operators must provide players with access to their data, with mandatory data portability and rectification rights.

PART X – AI USAGE

80. AI Usage Disclosure

All operators must provide the authority with a detailed description of all AI usage, including algorithms, data sources, and intended purposes.

81. Independent AI Audits

All AI systems must be independently audited for fairness, accuracy, and transparency, with mandatory audit reports and certifications.

82. AI Transparency

All AI systems must be transparent and explainable, with mandatory documentation and user-friendly interfaces.

83. Regular AI Updates

All AI systems must be regularly updated and monitored for performance, with mandatory version control and change management procedures.

PART XI - DORMANT ACCOUNTS AND UNCLAIMED WINNINGS

84. Dormant Account Policy

Operators must have a clear and transparent policy for dealing with dormant accounts, with mandatory notification procedures and timeframes.

85. Unclaimed Winnings Procedure

Operators must have a procedure for dealing with unclaimed winnings, with mandatory notification and return procedures.

86. Transfer to Authority

After a specified period, unclaimed winnings must be transferred to the Authority, with mandatory reporting and documentation.

PART XII - FINAL PROVISIONS

87. Severability

If any provision of this Act is found to be invalid or unenforceable by a court of competent jurisdiction, such invalidity shall not affect the remaining provisions, which shall continue in full force and effect.

88. Commencement and Enactment

This Act shall come into force on the date of its publication in the Official Gazette of Tuvalu.

89. Prior license

No licenses shall be deemed valid under this Act prior to its enactment.

90. Application submission starting date

The Tuvalu Gaming Authority shall commence accepting applications for online gaming licenses no later than sixty (60) days after the Act's official publication.

91. Regulation development

The Authority shall develop and publish additional regulations necessary for implementing this Act within ninety (90) days of its enactment.