# SMART CONTRACT AUDIT & LEGAL COMPLIANCE REPORT

Last Updated: February 25th, 2025

## 1. INTRODUCTION

This report provides an extensive technical and legal audit of the smart contracts used within MAGIC WORLD LTD, ensuring compliance with UK financial regulations, data protection laws, and global security standards. This audit examines the contract code, security vulnerabilities, regulatory considerations, and risk mitigation strategies to maintain a robust and compliant blockchain ecosystem.

MAGIC WORLD utilizes smart contracts for token issuance, in-game transactions, NFT ownership and decentralized interactions. This document highlights areas requiring legal and security safeguards to prevent regulatory breaches and security compromises.

## 2. TECHNICAL AUDIT

2.1 Code Review & Security Assessment

A comprehensive manual and automated review of the smart contracts was conducted to assess:

1. Code Efficiency & Accuracy: Ensures contract logic aligns with intended functionalities.
2. Security Vulnerability Testing: Identification of common blockchain threats.
3. Performance & Gas Optimization: Reduces transaction costs while maintaining security.
4. Access Control & Permissioning: Prevents unauthorized execution of critical functions.

Key security threats assessed:

1. Reentrancy Attacks: Protection against recursive function calls draining funds.
2. Integer Overflows/Underflows: Ensuring safe numeric calculations within contract execution.
3. Access Control & Privilege Escalation: Ensuring only authorized parties execute admin functions.
4. Denial-of-Service (DoS) Resistance: Preventing congestion exploits that impact contract functionality.
5. Immutability & Upgrade Mechanisms: Proper structuring to allow controlled upgrades without security compromises.

2.2 Smart Contract Code Audit Findings

1. Critical Issues: No critical security vulnerabilities were found.
2. High-Risk Issues: Implementing multi-signature authentication for administrative transactions is recommended.
3. Medium-Risk Issues: Optimize smart contract structure to reduce excessive gas consumption.
4. Low-Risk Issues: Enhance input validation to prevent unexpected contract behaviors.

Recommended Fixes:

1. Implement time-lock mechanisms on administrative functions to prevent instant exploitation.
2. Strengthen role-based access control (RBAC) for key functionalities.
3. Conduct ongoing monitoring and automated alerts for contract activity anomalies.

## 3. LEGAL COMPLIANCE REVIEW

3.1 UK Financial Conduct Authority (FCA) Compliance

1. Classification: The MAGIC WORLD Tokens are confirmed to be Utility Tokens, not securities under UK FCA guidelines (PS19/22).
2. Regulatory Exemptions: As non-securities, the tokens do not fall under FSMA 2000, but compliance with consumer protection laws is mandatory.
3. Future Considerations: Should token functionality change (e.g., introducing financial incentives), reassessment under FCA rules will be required.

3.2 UK GDPR & Data Protection Compliance

1. Personal Data Handling: The smart contract does not collect, store, or process personal user data, ensuring compliance with UK GDPR.
2. Blockchain & Right to Be Forgotten: Due to the immutable nature of blockchain, careful structuring of data off-chain is recommended.
3. Recommendations: Introduce zero-knowledge proof (ZKP) techniques for private transactions without exposing user identities.

3.3 Anti-Money Laundering (AML) & Know Your Customer (KYC)

1. KYC Implementation: Required for users interacting with regulated aspects of the MAGIC WORLD ecosystem (e.g., fiat-to-crypto transactions).
2. AML Requirements: Compliance with UK Money Laundering Regulations (MLR 2017) is necessary for all fiat-to-crypto gateways.
3. Risk Management: A risk-based approach should be adopted, ensuring automated monitoring for suspicious transactions.

## 4. RISK ASSESSMENT & MITIGATION STRATEGIES

4.1 Identified Risks

1. Regulatory Risks: Potential changes in UK crypto regulations could impact token utility or require additional compliance steps.
2. Security Risks: Risks of hacking, smart contract exploits, or external threats to the blockchain network.
3. Market Risks: Token value fluctuations due to external economic factors, regulatory shifts, or technological advancements.
4. Operational Risks: Errors in contract execution leading to financial loss or unintended contract behavior.

4.2 Recommended Mitigation Measures

1. Implement Automated Smart Contract Audits – Use third-party audit tools alongside manual reviews to detect vulnerabilities.
2. Regulatory Watch & Legal Reviews – Maintain an ongoing legal review process to ensure compliance with evolving FCA regulations.
3. Advanced Security Protocols – Introduce multi-layered authentication for high-value transactions.
4. User Education & Risk Disclosures – Provide transparent warnings to users about risks associated with blockchain transactions.

## 5. CONCLUSION & RECOMMENDATIONS

The MAGIC WORLD smart contracts have passed security and compliance assessments, confirming they are secure and legally compliant with UK FCA guidelines, UK GDPR, and AML/KYC regulations. However, to maintain long-term compliance:

1. Conduct bi-annual security audits to detect new vulnerabilities.
2. Update AML/KYC policies as needed to align with UK regulatory changes.
3. Implement user-friendly compliance reporting to improve transparency for token holders.
4. Continue monitoring UK FCA guidelines for any changes impacting token utility.

For further legal inquiries, contact: support@magicworld.com.