bearerCORE™

Sovereign CBDC Infrastructure Platform

Comprehensive Legal Framework & Liability Protection Structure

---

Prepared for: TowerPoint Group, Ltd.

Platform: bearerCORE™

Classification: Sovereign CBDC Infrastructure Framework

Version: Draft 1.0

Effective: January 2026

Jurisdiction: Republic of Ghana · African Union · International

IMPORTANT NOTICE

This document is a strategic legal framework outline intended to support the development of a comprehensive sovereign infrastructure legal package for bearerCORE™. This framework should be reviewed and finalized by qualified international technology, financial regulatory, central bank regulatory, data privacy, cross-border payments, and cybersecurity counsel. This document does not constitute legal advice.

This document constitutes the Comprehensive Legal Framework for the bearerCORE™ platform.

1 Introduction

bearerCORE™ is a sovereign CBDC infrastructure platform designed to support:

- Central Bank Digital Currencies (CBDCs)
- National settlement systems
- Tokenized sovereign assets
- Regulated digital payment rails
- Interoperable financial infrastructure
- Cross-border digital settlement environments
- Digital monetary infrastructure modernization

TowerPoint Group, Ltd. acts solely as a technology infrastructure provider and does not function as:

- A deposit-taking institution
- A money transmitter
- A commercial bank
- A custodian of sovereign currency
- A securities exchange
- A fiduciary
- An investment advisor
- A financial intermediary

2 Core Legal Objectives

The legal framework should be structured to:

1. Minimize operational liability exposure
2. Protect against sovereign misuse claims
3. Limit software warranty obligations
4. Establish infrastructure-provider status only
5. Protect against indirect financial loss claims
6. Protect against cyber-event litigation
7. Clarify jurisdictional boundaries
8. Protect intellectual property
9. Define central bank responsibilities
10. Define participant obligations
11. Limit force majeure exposure
12. Limit consequential damages
13. Define arbitration procedures
14. Clarify infrastructure limitations
15. Establish sovereign implementation responsibility

3 Definitions

3.1 Key Terms

"Platform" Means the bearerCORE™ software stack, APIs, settlement infrastructure, cryptographic systems, gateways, middleware, documentation, and associated technical infrastructure.

"Central Bank" Means the sovereign monetary authority or designated governmental institution implementing the bearerCORE™ infrastructure.

"Participant" Means any regulated institution, authorized entity, financial institution, or approved operator utilizing the infrastructure.

"Digital Asset" Means any digital representation of value processed through the infrastructure.

"Infrastructure Services" Means software, APIs, network services, interoperability mechanisms, validation systems, or associated technical services.

"Force Majeure Event" Means any event beyond the reasonable control of TowerPoint Group, Ltd., including but not limited to:

- War
- Terrorism
- Cyber warfare
- State-sponsored cyber attacks
- Internet outages
- Satellite failures
- DNS failures
- Regulatory intervention
- Government shutdowns
- Electrical grid collapse
- Telecommunications failures
- Civil unrest
- Pandemic events
- Natural disasters
- Blockchain protocol failures
- Cryptographic compromise events
- Third-party cloud provider outages
- Distributed denial-of-service attacks
- Undersea cable failures
- International sanctions
- Cross-border banking disruptions
- Currency crises
- Digital asset market collapse
- AI-driven cyber attacks

- Quantum-computing cryptographic compromise

4 Liability Limitation Structure

4.1 Infrastructure Provider Status

TowerPoint Group, Ltd. provides software and infrastructure services only.

TowerPoint Group, Ltd.:

- does not control sovereign monetary policy;
- does not issue sovereign currency;
- does not control monetary supply;
- does not guarantee transaction settlement;
- does not guarantee uninterrupted system availability;
- does not assume fiduciary obligations;
- does not guarantee interoperability with third-party systems;
- does not guarantee regulatory acceptance;
- does not guarantee operational continuity of participating institutions.

4.2 Exclusion of Financial Liability

Under no circumstances shall TowerPoint Group, Ltd. be liable for:

- monetary loss;
- indirect damages;
- consequential damages;
- sovereign reserve losses;
- transaction reversals;
- monetary policy failures;
- exchange rate fluctuations;
- liquidity crises;
- digital asset volatility;
- banking failures;
- central bank operational failures;
- participant misconduct;
- unauthorized access events;
- key compromise events;
- smart contract vulnerabilities;
- blockchain forks;
- validator failures;
- cyber attacks;
- data corruption;
- telecommunications outages;

- cloud infrastructure failures;
- sanctions-related interruptions;
- geopolitical disruptions;
- legal or regulatory changes.

4.3 Maximum Liability Cap

To the maximum extent permitted by law:

The aggregate liability of TowerPoint Group, Ltd. shall not exceed:

- the fees paid for the applicable infrastructure services during the preceding twelve (12) month period; OR
- a contractually defined cap negotiated with the sovereign entity.

5 Technical Disclaimers

5.1 No Warranty Disclaimer

The bearerCORE™ platform is provided "AS IS," "AS AVAILABLE," without warranties of any kind, including but not limited to:

- merchantability;
- fitness for a particular purpose;
- uninterrupted availability;
- error-free operation;
- non-infringement;
- cybersecurity resilience;
- compatibility with third-party systems;
- continuous interoperability.

5.2 Blockchain & Cryptographic Risk Disclaimer

Users acknowledge that:

- blockchain systems carry inherent risk;
- cryptographic systems may evolve over time;
- quantum computing developments may affect encryption standards;
- digital asset systems may experience unforeseen vulnerabilities;
- decentralized systems may fork or fragment;
- consensus mechanisms may fail.

5.3 AI & Automation Disclaimer

Where AI-assisted monitoring, analytics, fraud detection, or automation systems are utilized:

- outputs may be probabilistic;
- false positives may occur;
- no AI decisioning system is guaranteed accurate;
- sovereign authorities remain responsible for final policy decisions.

5.4 Regulatory Disclaimer

TowerPoint Group, Ltd. does not guarantee:

- future regulatory approval;
- cross-border legality;
- tax treatment;
- licensing outcomes;
- securities-law classifications;
- anti-money laundering compliance determinations.

6 Data Privacy & Sovereignty

6.1 Privacy by Design

bearerCORE™ is designed to minimize the collection of personally identifiable information.

6.2 Data Sovereignty

Each sovereign entity remains responsible for:

- data residency requirements;
- sovereign data governance;
- retention obligations;
- lawful interception compliance;
- national cybersecurity requirements.

6.3 Non-Custodial Infrastructure

TowerPoint Group, Ltd. does not:

- hold customer funds;
- control private keys;
- custody sovereign reserves;
- manage end-user wallets unless explicitly agreed by separate written agreement.

7 Intellectual Property Protection

7.1 Ownership

All bearerCORE™ intellectual property remains the exclusive property of TowerPoint Group, Ltd., including:

- source code;
- APIs;
- cryptographic systems;
- documentation;
- protocols;
- architecture;
- trademarks;

- patents;
- trade secrets;
- interoperability systems.

7.2 Restrictions

No party may:

- reverse engineer;
- decompile;
- replicate;
- redistribute;
- sublicense;
- modify;
- extract proprietary logic;
- create derivative systems

without written authorization.

8 Confidentiality

All technical documentation, architecture diagrams, APIs, specifications, source code, deployment procedures, and interoperability frameworks shall be treated as confidential information.

9 Cybersecurity & Incident Response

9.1 Shared Responsibility Model

Cybersecurity responsibilities shall be shared among:

- sovereign authorities;
- participating institutions;
- hosting providers;
- network operators;
- TowerPoint Group, Ltd.

9.2 No Absolute Security Guarantee

No system can guarantee absolute immunity from:

- cyber attacks;
- insider threats;
- zero-day exploits;
- advanced persistent threats;
- state-sponsored attacks.

10 Force Majeure

Neither party shall be liable for delays or failures caused by force majeure events.

Force majeure shall include:

- acts of war;
- terrorism;
- insurrection;
- sanctions;
- cyber warfare;
- sovereign debt crises;
- banking collapses;
- electrical outages;
- telecommunications failures;
- cloud outages;
- internet instability;
- blockchain instability;
- software supply-chain attacks;
- AI-generated cyber events;
- pandemics;
- natural disasters.

11 Arbitration & Dispute Resolution

11.1 Governing Law

Recommended governing law jurisdictions may include, based on transaction structure:

- England & Wales
- Singapore
- Switzerland
- Dubai International Financial Centre (DIFC)
- Mauritius

11.2 Arbitration

All disputes shall be resolved exclusively through confidential binding arbitration. Recommended arbitration forums:

- London Court of International Arbitration (LCIA)
- International Chamber of Commerce (ICC)
- Singapore International Arbitration Centre (SIAC)
- Dubai International Arbitration Centre (DIAC)

11.3 Waiver of Jury Trial

All parties waive any right to trial by jury.

11.4 Sovereign Immunity

Any sovereign entity utilizing the infrastructure shall explicitly define any sovereign immunity waivers within the governing agreement.

12 Compliance Frameworks

The platform may align with:

- GDPR principles
- AU Malabo Convention
- Ghana Data Protection Act
- FATF guidance
- ISO 27001
- ISO 20022
- NIST Cybersecurity Framework
- CBDC interoperability standards

13 Export Control & Sanctions

Users acknowledge that certain technologies may be subject to:

- export control laws;
- sanctions restrictions;
- anti-money laundering obligations;
- anti-terrorism financing regulations.

14 Survival Clauses

The following provisions survive termination:

- confidentiality;
- intellectual property;
- liability limitations;
- indemnification;
- arbitration;
- dispute resolution;
- governing law.

15 Next Phase Documents to Develop

Recommended Full Legal Package

A. Terms of Service Full sovereign infrastructure platform terms.

B. Master Services Agreement (MSA) Central bank enterprise agreement.

C. Sovereign Infrastructure License Agmt. Sovereign CBDC infrastructure licensing.

D. Privacy Policy Operational privacy framework.

E. Security & Cryptographic Disclosure Technical security disclosures.

F. Regulatory Cooperation Framework Cross-border cooperation procedures.

G. Incident Response & Cybersecurity Operational security governance.

H. Central Bank Deployment Agreement Implementation-specific CBDC deployment framework.

I. API Usage & Developer Terms Third-party integration governance.

J. Whitepaper Risk Disclosure Appendix Public-facing risk disclosure documentation.

16 Strategic Recommendation

Before production deployment or central bank onboarding, TowerPoint Group, Ltd. should engage:

- international fintech counsel;
- sovereign regulatory counsel;
- cross-border payments counsel;
- cybersecurity counsel;
- export-control counsel;
- sanctions counsel;
- intellectual property counsel.

A jurisdictional strategy should also be developed for:

- entity structuring;
- IP holding entities;
- arbitration jurisdiction;
- licensing structure;
- data residency;
- regulatory segmentation.

END OF DOCUMENT

This document constitutes the Comprehensive Legal Framework for the bearerCORE™ platform. Questions or institutional enquiries should be directed to TowerPoint Group, Ltd. via the Protocol Desk at bearercore.com/protocol-desk.