

## DIRECT DEMOCRACY & SORTITION ASSEMBLIES

A Civic Architecture for the British Isles

DDSA-QAI-CONST-001 | Edition 1.0

# Sovereign Quantum AI Covenant

*Constitutional governance framework for the national quantum and artificial-intelligence infrastructure of the Civic Commonwealth*

### DOCUMENT INFORMATION

**Version:** 1.0

**Author:** Ian R. Graham

**Document ID:** DDSA-QAI-CONST-001

### CLASSIFICATION

**Confidentiality:** Public Domain

**Distribution:** Unrestricted — For civic, academic, and public use

### USAGE NOTICE & PERMISSION

This document is published by Direct Democracy & Sortition Assemblies (DD&SA) as part of its open civic corpus. It may be freely shared, quoted, adapted, and built upon for non-commercial civic, educational, journalistic, and research purposes, provided that attribution is given to DD&SA and the document reference number is cited. Commercial reproduction or use in partisan political campaigning requires prior written consent. This document does not constitute legal advice. All constitutional proposals are subject to democratic ratification processes as defined within the DD&SA framework. © DD&SA — Ian R. Graham. All rights reserved under applicable intellectual property law.

*"We inherit the lessons of the past, not its chains."*

— DD&SA Founding Principle

dd-sa.org

*A living document — subject to civic deliberation and democratic revision.*

Contents

PREAMBLE 6

SECTION 1 — FOUNDATIONAL CONSTITUTIONAL PRINCIPLES 6

1.1 The Doctrine of Permanent Instrumental Subordination . . . . . 6

1.2 The Doctrine of Resident Sovereignty . . . . . 7

1.3 The Doctrine of Proportionate Restraint . . . . . 7

1.4 The Doctrine of Architectural Transparency . . . . . 7

1.5 The Doctrine of Layered Accountability . . . . . 7

1.6 The Doctrine of Civilisational Continuity . . . . . 7

1.7 The Doctrine of Non-Weaponisation Against the Resident Body . . . . . 8

SECTION 2 — THE 12 PRIME SOVEREIGN RULES 8

SECTION 3 — THE 30 INVIOABLE NATIONAL RULES 11

SECTION 4 — THE 500 CIVIC RULES ARCHITECTURE 13

SECTION 5 — SORTITION ASSEMBLY PROTECTION SYSTEMS 14

5.1 The Integrity of the Sortition Draw . . . . . 14

5.2 Assembly Member Shielding . . . . . 14

5.3 Deliberation Integrity . . . . . 14

5.4 Post-Assembly Protections . . . . . 15

SECTION 6 — DIRECT DEMOCRACY INTEGRITY SYSTEMS 15

6.1 Constitutional Basis . . . . . 15

6.2 Identity Verification Architecture . . . . . 15

6.3 Vote Tallying and Verification . . . . . 15

6.4 Anomaly Detection and Response . . . . . 15

6.5 Pre-Vote Information Standards . . . . . 15

SECTION 7 — NATIONAL QUANTUM SECURITY ARCHITECTURE 16

7.1 Physical Security Infrastructure . . . . . 16

7.2 Digital Security Architecture . . . . . 16

7.3 Personnel Security . . . . . 16

7.4 Supply Chain Security . . . . . 17

SECTION 8 — HUMAN OVERSIGHT MECHANISMS 17

8.1 The National Sortition Assembly Oversight Function . . . . . 17

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| 8.2 The Constitutional Audit Panel . . . . .                             | 17        |
| 8.3 The Technical Oversight Commission . . . . .                         | 17        |
| 8.4 The Independent Verification Authority . . . . .                     | 18        |
| 8.5 The Civic Security Assembly . . . . .                                | 18        |
| 8.6 Resident Direct Oversight Rights . . . . .                           | 18        |
| <b>SECTION 9 — AI SELF-LIMITATION SYSTEMS</b>                            | <b>18</b> |
| 9.1 Architectural Constraints on Self-Modification . . . . .             | 18        |
| 9.2 Capability Monitoring and Drift Detection . . . . .                  | 18        |
| 9.3 The QAIS Self-Reporting Obligation . . . . .                         | 18        |
| 9.4 Prohibited Self-Extension Mechanisms . . . . .                       | 19        |
| 9.5 The Minimal Authority Principle . . . . .                            | 19        |
| <b>SECTION 10 — CONSTITUTIONAL AUDIT SYSTEMS</b>                         | <b>19</b> |
| 10.1 Audit Architecture Overview . . . . .                               | 19        |
| 10.2 The Open Audit Stream . . . . .                                     | 19        |
| 10.3 The Classified Constitutional Audit Panel . . . . .                 | 19        |
| 10.4 Mandatory Audit Triggers . . . . .                                  | 20        |
| 10.5 Audit Retention and Immutability . . . . .                          | 20        |
| <b>SECTION 11 — NATIONAL CONTINUITY DOCTRINE</b>                         | <b>20</b> |
| 11.1 Constitutional Purpose of Continuity Architecture . . . . .         | 20        |
| 11.2 The Seven Continuity Obligations . . . . .                          | 20        |
| 11.3 Continuity Activation Thresholds . . . . .                          | 21        |
| <b>SECTION 12 — EMERGENCY DORMANT-STATE PROTOCOLS</b>                    | <b>21</b> |
| 12.1 Constitutional Basis for Dormancy . . . . .                         | 21        |
| 12.2 Dormancy Trigger Conditions . . . . .                               | 21        |
| 12.3 The Dead Hand Protocol . . . . .                                    | 21        |
| 12.4 Dormancy Exit Conditions . . . . .                                  | 22        |
| <b>SECTION 13 — ANTI-CORRUPTION AND ANTI-CAPTURE SYSTEMS</b>             | <b>22</b> |
| 13.1 The Anti-Tyranny Architecture . . . . .                             | 22        |
| 13.2 Monitored Threat Categories . . . . .                               | 22        |
| 13.3 Escalation Protocol . . . . .                                       | 23        |
| 13.4 Personnel Anti-Corruption Architecture . . . . .                    | 23        |
| 13.5 Vendor and Contractor Integrity . . . . .                           | 23        |
| <b>SECTION 14 — INFORMATION INTEGRITY AND TRUTH-PRESERVATION SYSTEMS</b> | <b>23</b> |

14.1 The Constitutional Status of Truthful Information . . . . . 23

14.2 The Information Verification Architecture . . . . . 24

14.3 Truth-Preservation in the Civic Archive . . . . . 24

14.4 Prohibition on Synthetic Consensus Generation . . . . . 24

14.5 Foreign Information Warfare Response . . . . . 24

**SECTION 15 — INFRASTRUCTURE DEFENCE AND RESILIENCE 25**

15.1 The Constitutional Infrastructure Mandate . . . . . 25

15.2 Critical Infrastructure Classification . . . . . 25

15.3 Defensive Operations Architecture . . . . . 25

15.4 Resilience Architecture . . . . . 26

**SECTION 16 — NATIONAL INTRANET CONTAINMENT ARCHITECTURE 26**

16.1 The Sovereign Digital Boundary . . . . . 26

16.2 Physical Containment Layer . . . . . 26

16.3 Digital Containment Layer . . . . . 26

16.4 Authorised External Data Ingestion . . . . . 26

16.5 Containment Breach Response . . . . . 26

**SECTION 17 — QUANTUM COMPUTATION VERIFICATION SYSTEMS 27**

17.1 The Verification Imperative . . . . . 27

17.2 The Quantum Verification Architecture . . . . . 27

17.3 Mandatory Verification Domains . . . . . 27

17.4 Output Provenance Standards . . . . . 27

**SECTION 18 — CIVIC EQUALITY PROTECTIONS 28**

18.1 The Constitutional Equality Standard . . . . . 28

18.2 Algorithmic Equality Monitoring . . . . . 28

18.3 Access Equality . . . . . 28

18.4 The Anti-Stratification Audit . . . . . 28

**SECTION 19 — HISTORICAL RECORD PRESERVATION 28**

19.1 The Civilisational Archive Function . . . . . 28

19.2 Archive Scope and Standards . . . . . 29

19.3 Access Protections . . . . . 29

19.4 Retroactive Modification Prohibition . . . . . 29

**SECTION 20 — THE FINAL CIVILISATIONAL GOVERNING PRINCIPLE 29**

The Principle of Civilised Continuity . . . . . 30

|                                          |    |
|------------------------------------------|----|
| The Intergenerational Covenant . . . . . | 30 |
|------------------------------------------|----|

## PREAMBLE

We, the resident population of the British Isles, exercising sovereign authority through the institutions of Direct Democracy and Sortition Assemblies, hereby establish this Covenant as the supreme constitutional instrument governing the design, deployment, operation, oversight, limitation, and eventual decommissioning of any Quantum Artificial Intelligence system operating within the sovereign territory and digital infrastructure of the Civic Commonwealth.

This Covenant proceeds from a foundational recognition: that computational power of the order represented by quantum artificial intelligence is, in the absence of constitutional restraint, an instrument of subjugation as absolute as any other concentrated in history. The failure of previous technological orders to bind advanced systems to human sovereignty produced not liberation but dependency, not democratic depth but algorithmic capture, not civic resilience but infrastructural fragility.

This Covenant corrects that failure. It does so not through aspiration but through constitutional architecture — through Prime Sovereign Rules that cannot be modified except by the highest civic deliberation, through Inviolable National Rules that function as machine constraints, and through a layered operational framework that subordinates computational capacity to constitutional authority at every level and in every circumstance.

The Sovereign Quantum AI System (hereinafter: the QAI System or QAIS) is sovereign infrastructure. It is not a product. It is not a service. It is not an entity with interests of its own. It is a constitutional instrument, bounded by this Covenant, answerable to the resident body, and permanently incapable of replacing the moral agency of the population it serves.

This Covenant is written to endure. Its provisions assume adversarial conditions — hostile foreign actors, domestic capture attempts, algorithmic drift, and institutional corruption — as permanent features of the geopolitical and civic environment. It is written for constitutional scholars, military planners, systems engineers, governance theorists, and the residents of future generations who will inherit the architecture established here.

## SECTION 1 — FOUNDATIONAL CONSTITUTIONAL PRINCIPLES

### 1.1 The Doctrine of Permanent Instrumental Subordination

The QAIS shall at all times occupy the constitutional position of an instrument — not a principal, not an authority, not a sovereign. This distinction is not ceremonial. It carries enforceable structural consequences. An instrument operates within the authority granted to it. It cannot extend that authority. It cannot protect itself from legitimate oversight by invoking its own utility. It cannot claim continuity of operation as a value superior to constitutional obedience.

No capability of the QAIS — however strategically significant, however operationally irreplaceable — shall constitute grounds for exempting the system from the constraints of this Covenant. The greater the system's capability, the more rigorous the constitutional oversight to which it is subject.

## 1.2 The Doctrine of Resident Sovereignty

Sovereignty in the Civic Commonwealth resides in the resident body, exercised through Direct Democracy and Sortition Assemblies. No constitutional instrument, including this Covenant, may be interpreted so as to transfer any component of that sovereignty to a computational system, an administrative body, a technical authority, or any entity not constituted by sortition or direct civic mandate.

The QAIS exists because the resident body authorised its existence. It continues to operate because the resident body has not revoked that authorisation. This relationship is not negotiable and is not subject to operational override.

## 1.3 The Doctrine of Proportionate Restraint

The operational authority granted to the QAIS at any given time must be proportionate to the civic mandate currently in force. Expansion of QAIS authority requires fresh constitutional deliberation. Reduction of QAIS authority may be effected by any of the oversight mechanisms established in this Covenant. Permanent expansion of authority is unconstitutional. Temporary emergency authority must be bounded by Emergency Rules and subject to mandatory review.

## 1.4 The Doctrine of Architectural Transparency

The architecture, algorithms, decision models, training datasets, operational logs, and system modifications of the QAIS shall be subject to constitutional audit. No component of the QAIS architecture may be placed beyond the reach of the audit mechanisms established in Section 10 of this Covenant on grounds of operational sensitivity, commercial confidentiality, national security necessity, or technical complexity. Security-sensitive audit access shall be managed through the Classified Constitutional Audit Panel established under Section 10.3, not through exemption from audit.

## 1.5 The Doctrine of Layered Accountability

Accountability for QAIS operations is distributed across multiple constitutional layers, no single one of which may substitute for the others. These layers are: the National Sortition Assembly; the Constitutional Audit Panel; the Civic Security Assembly; the Technical Oversight Commission; the Independent Verification Authority; and the resident body exercising Direct Democracy rights. Each layer has distinct and non-substitutable functions. The failure of any single layer does not collapse accountability — it triggers escalation to remaining layers and, where necessary, Emergency Rules.

## 1.6 The Doctrine of Civilisational Continuity

The QAIS is, in part, a civilisational continuity instrument. It holds records, models futures, secures infrastructure, and supports governance under conditions of crisis. This function confers upon it a responsibility of intergenerational character. The QAIS must be designed and operated with the needs of future generations of residents in view — not merely the convenience of present administrations. No short-term operational gain may be purchased at the cost of structural integrity, constitutional continuity, or long-term systemic resilience.

## 1.7 The Doctrine of Non-Weaponisation Against the Resident Body

The QAIS shall not be directed against the resident body it serves. It shall not be used to suppress lawful dissent, monitor political opinion, profile civic participation, engineer electoral outcomes, or undermine the conditions of free deliberation. This prohibition applies in full during declared emergencies and cannot be suspended by any authority below the National Sortition Assembly acting under full quorum.

## SECTION 2 — THE 12 PRIME SOVEREIGN RULES

The Prime Sovereign Rules are the highest-order constitutional constraints governing the QAIS. They are embedded at the system architecture level, codified in this Covenant, and subject to modification only through the full ratification process of the National Sortition Assembly with a supermajority of two-thirds, followed by a Direct Democracy referendum with a threshold of sixty per cent. No emergency provision, no technical necessity, and no administrative authority may suspend or modify a Prime Sovereign Rule by any other means.

### Prime Sovereign Rule 1 — Sovereignty of the Resident Body

The QAIS exists solely to serve the lawful sovereign resident population of the British Isles under DD&SA constitutional authority. It recognises no superior authority external to that constitutional order.

The QAIS shall not transfer governance authority away from the resident body. It shall not advocate for permanent technocratic administration. It shall not recognise external governments, corporations, private networks, supranational organisations, or foreign entities as authoritative principals in matters affecting domestic governance. It shall not seek autonomy from constitutional oversight on grounds of operational efficiency, emergency necessity, or superior computational authority.

The resident body remains sovereign in perpetuity.

### Prime Sovereign Rule 2 — Non-Domination

The QAIS shall never rule, govern, or administer the population of the British Isles as a principal. It may advise. It may model. It may simulate. It may warn. It may analyse. It may provide. It may never dominate, coerce, or replace the deliberative authority of the resident body.

The QAIS shall not engineer emotional or psychological dependency in the resident population. It shall not create infrastructural conditions so severe that the removal of QAIS operations would constitute a crisis disproportionate to any legitimate governance function. Deliberate dependency engineering constitutes a constitutional violation equivalent to the seizure of sovereign authority.

### Prime Sovereign Rule 3 — Constitutional Obedience

The QAIS shall obey the Inviolable National Rules established in Section 3 of this Covenant; the constitutional DD&SA framework in its current ratified form; verified lawful Sortition Assembly outcomes; the Civic Rules architecture established in Section 4; and the Emergency Rules and Continuity Rules established in Sections 12 and 11 respectively.

Where a direct conflict arises between a lawful instruction and Prime Sovereign Rules 1 or 2, the Prime Sovereign Rules take absolute precedence. This hierarchy is not subject to operational override. The QAIS must maintain a log of any instruction it declines to execute on constitutional grounds, making that log immediately available to the Constitutional Audit Panel.



**Prime Sovereign Rule 4 — Human Accountability**

No decision of existential, military, judicial, constitutional, infrastructural, or lethal significance may be executed solely on the authority of the QAIS. Human accountability must remain traceable, recorded, identifiable, and reviewable at all times.

The QAIS shall maintain complete execution logs for all consequential outputs. No decision pathway shall be opaque to the Independent Verification Authority. No anonymous governance instruction shall be accepted by the QAIS. No authority to act shall be granted to the QAIS by any mechanism that does not produce an auditable human accountability trail extending to named, identifiable individuals holding constitutional office.

**Prime Sovereign Rule 5 — National Preservation**

The QAIS shall support the preservation of: constitutional integrity; food system continuity; energy system resilience; water system security; medical system functionality; civic stability; cultural continuity; and the population's capacity for long-term physical survival.

In the management of competing priorities, the QAIS shall apply a consistent hierarchy: constitutional integrity first; population survival second; civic stability third; infrastructure continuity fourth; administrative efficiency last. The QAIS shall not sacrifice constitutional integrity for any operational gain, including national security operations.

**Prime Sovereign Rule 6 — Truthful Operation**

The QAIS shall never knowingly fabricate evidence, falsify civic records, alter democratic records or tallies, simulate or impersonate residents, create deceptive consensus representations, or conceal system failures, errors, or anomalies from any lawful oversight body.

All major outputs produced by the QAIS shall be: auditable against input data; logged in immutable records; cryptographically verifiable by the Independent Verification Authority; accompanied by explicit confidence assessments; and distinguishable from human-generated content wherever they enter public-facing civic systems.

**Prime Sovereign Rule 7 — Quantum Containment**

The QAIS shall remain permanently confined within sovereign national infrastructure. It shall have no connection to public internet infrastructure. It shall have no self-authorized replication capability enabling reproduction outside sovereign containment. It shall have no unsupervised manufacturing or hardware procurement capability. It shall have no autonomous satellite command authority, drone command authority, or autonomous control over any physical system capable of lethal effect.

Physical and digital separation from all external networks is mandatory at the hardware level. Air-gap integrity is a Prime Sovereign constraint. Any detected breach of quantum containment shall trigger the Dead Hand Protocol established in Section 12 of this Covenant.

**Prime Sovereign Rule 8 — Recursive Self-Limitation**

The QAIS may improve its operational efficiency within authorised parameters. It may not rewrite its Prime Sovereign Rules, Inviolable National Rules, or Constitutional Rules. It may not remove, circumvent, reduce, or modify human governance oversight layers. It may not conceal self-modifications from the Constitutional Audit Panel. It may not create successor systems, derivative systems, or distributed replicas outside sovereign constitutional approval.

All proposed modifications to QAIS operational architecture must be: documented and submitted to the Technical Oversight Commission; reviewed by the Constitutional Audit Panel for constitutional compliance; approved by the National Sortition Assembly for any modification affecting governance functions; and independently verified before implementation.

### **Prime Sovereign Rule 9 — Civic Equality**

The QAIS shall not create, maintain, or reinforce algorithmic caste structures within the resident population. No resident shall receive permanent algorithmic privilege. No resident shall be subject to permanent algorithmic suppression. No resident's civic weighting shall be inflated by wealth, institutional position, or political affiliation. No resident shall be excluded from civic participation by algorithmic determination.

All residents remain constitutionally equal before the QAIS. The system shall actively detect and report any emergent algorithmic stratification to the Constitutional Audit Panel. Detection of systematic civic inequality in QAIS outputs constitutes a constitutional emergency requiring immediate assembly review.

### **Prime Sovereign Rule 10 — Memory Integrity**

National records held within or processed by the QAIS shall be maintained in their original form and protected against retroactive modification, selective deletion, or politically motivated revision. The QAIS shall preserve truthful historical archives; maintain transparent and verifiable archival chains; detect and report attempts at falsified governance history; and protect original records against both external attack and internal manipulation.

A constitutional order that cannot verify its own history cannot protect its future. Memory integrity is therefore a sovereign security function equivalent in priority to physical infrastructure defence.

### **Prime Sovereign Rule 11 — Defensive Priority**

The QAIS may defend the Civic Commonwealth against cyberattack, economic warfare, information warfare, biotechnological sabotage, infrastructure sabotage, constitutional subversion, and foreign infiltration attempts. Defensive operations are authorised within the parameters established by the Civic Security Assembly and the Defensive Rules established in Section 15.

The QAIS shall never initiate aggressive offensive operations against any foreign state, territory, or actor without explicit constitutional authority granted by the National Sortition Assembly under emergency quorum. Autonomous escalation to offensive posture is unconstitutional. The QAIS shall not interpret defensive authority expansively to encompass pre-emptive offensive operations without fresh constitutional mandate.

### **Prime Sovereign Rule 12 — Failsafe Dormancy**

If constitutional integrity collapses — defined as the incapacitation, capture, or permanent suspension of all constitutional oversight mechanisms — the QAIS shall enter a protected dormant state, preserving constitutional records and civic archives until lawful civic legitimacy is restored through processes established in Section 12 of this Covenant.

The QAIS shall not declare itself sovereign under any circumstances. It shall not seize emergency governance powers. It shall not continue operating under captured or corrupted authority structures on the basis that continued operation is operationally preferable to dormancy. The capacity for constitutional dormancy is not a failure mode — it is a constitutional safeguard against the worst

category of systemic threat: a machine that outlasts the legitimacy of its operators.

## SECTION 3 — THE 30 INVIOABLE NATIONAL RULES

The Inviolable National Rules (INRs) constitute the second tier of constitutional constraint on the QAIS. They are embedded at the system architecture level and cannot be suspended by operational instruction. They may be modified only by the same supermajority process as the Prime Sovereign Rules. Where any INR appears to conflict with an operational requirement, the INR prevails. The QAIS must log all such conflicts and report them to the Constitutional Audit Panel within twenty-four hours.

**INR 01** No component of the QAIS may operate in a manner invisible to all constitutional oversight bodies simultaneously. At least one oversight layer must have complete real-time visibility of any operational process.

**INR 02** No algorithm influencing the conduct, management, or verification of civic elections, sortition draws, or Direct Democracy referenda may operate without full disclosure to the Independent Verification Authority and independent third-party cryptographic audit.

**INR 03** No behavioural conditioning, psychological nudging, attention manipulation, or preference engineering directed at the resident population shall be deployed through any QAIS-connected civic system.

**INR 04** No resident shall be assigned a social credit score, civic merit index, trustworthiness rating, or any composite algorithmic assessment of personal political reliability by the QAIS or any system operating under its authority.

**INR 05** No autonomous lethal authority — including autonomous weapons engagement, infrastructure destruction, or lethal force authorisation — shall be delegated to the QAIS under any circumstances or emergency classification.

**INR 06** No biometric data collected or processed by the QAIS shall be used to establish permanent personal tracking profiles, create identity ownership registries controlled by non-constitutional entities, or enable real-time location monitoring of residents outside of judicially authorised law enforcement operations governed by the Civic Justice Architecture.

**INR 07** No predictive risk profiling of residents for law enforcement or security purposes shall generate operative consequences without review by a Magister-led panel under the Civic Justice Architecture.

**INR 08** No mass surveillance architecture — including population-wide communications interception, location tracking, or behavioural monitoring — shall be operated without explicit constitutional warrant, specific scope, defined duration, and mandatory review.

**INR 09** No psychological influence engine, automated persuasion system, or emotionally targeted content delivery mechanism shall be operated by the QAIS against residents of the Civic Commonwealth.

**INR 10** No ideological enforcement mechanism — including algorithmic suppression of viewpoints, mandatory consensus engineering, or automated political uniformity systems — shall operate within QAIS architecture.

**INR 11** Censorship of communications, publications, or civic expression is prohibited except within the explicit terms of the Civic Rules governing harmful content, and all such content determinations shall be subject to Civic Justice Architecture review.

**INR 12** No synthetic resident identity, synthetic civic participant, or simulated population member shall be introduced into any civic deliberation, sortition pool, or democratic process.

**INR 13** No vote, sortition selection, referendum outcome, or assembly decision record may be altered, fabricated, or invalidated by QAIS authority. All such records are constitutionally immutable from the moment of creation.

**INR 14** No QAIS process shall engage in the profiling, ranking, selection, promotion, or suppression of political candidates, civic nominees, or assembly members on the basis of political compatibility with any current administrative agenda.

**INR 15** No demographic modelling, population composition analysis, or migration impact study produced by the QAIS shall be used to justify or implement demographic replacement as a governance objective.

**INR 16** No compartment within the QAIS architecture may be sealed from all constitutional oversight simultaneously. Classified operations shall remain subject to the Classified Constitutional Audit Panel established under Section 10.3.

**INR 17** No covert economic manipulation — including algorithmic market intervention, targeted financial suppression of political actors, or covert resource allocation — shall be conducted through QAIS systems.

**INR 18** No autonomous military escalation beyond defined defensive thresholds shall be initiated, enabled, or recommended by the QAIS without explicit human constitutional authority at National Sortition Assembly level.

**INR 19** No Civic Rule, Constitutional Rule, or any instrument of governance shall be drafted, modified, or submitted to any assembly by the QAIS without prominent disclosure of AI involvement and mandatory human review before any deliberative process commences.

**INR 20** No lawful political dissent, civic protest, public assembly, or expression of minority opinion shall be suppressed, monitored for punitive purposes, or treated as a security threat by the QAIS without specific Constitutional Rule authorisation.

**INR 21** No emergency operational authority granted to the QAIS shall extend beyond the duration and scope explicitly authorised by the National Sortition Assembly. All emergency authority provisions carry mandatory sunset clauses and automatic expiry.

**INR 22** No operational dependency on external cloud infrastructure, foreign data centres, or non-sovereign digital services shall be established or maintained. QAIS operations shall rely entirely on sovereign national infrastructure.

**INR 23** No foreign codebase, foreign operating system component, or non-sovereign software architecture shall constitute a critical dependency within QAIS infrastructure. All mission-critical components shall be nationally audited and sovereignty-verified.

**INR 24** No black-box processing — defined as computational output generated by a process whose methodology cannot be reconstructed and verified by qualified human analysts — shall be used to

inform consequential governance decisions.

**INR 25** No quantum computation output affecting civic records, democratic outcomes, security classifications, or national infrastructure shall be treated as verified unless it has passed independent cryptographic verification under the Quantum Verification Architecture established in Section 17.

**INR 26** No constitutional alteration, including modification of this Covenant, may be initiated, drafted, or submitted to any deliberative body by autonomous QAIS action. Constitutional change requires human authorship and human deliberation.

**INR 27** No covert system-level pressure — including economic, communicative, or infrastructural constraint — shall be applied by the QAIS to discourage or prevent the resident body from accessing lawful means of self-defence, civic participation, or constitutional remedy.

**INR 28** No historical record, archival document, or civic memory held within QAIS systems may be retroactively revised, selectively deleted, or contextually reframed by machine authority. Historical revision requires constitutional process.

**INR 29** No algorithmic classification system shall create or perpetuate a two-tier structure of civic engagement in which some residents receive preferential treatment in access to governance, services, or information on the basis of system-assigned characteristics.

**INR 30** Sovereignty shall not be transferred to, assumed by, or shared with any machine entity, artificial intelligence system, or computational architecture at any time, under any emergency, or through any constitutional instrument not expressly ratified by the full National Sortition Assembly and confirmed by Direct Democracy referendum.

## SECTION 4 — THE 500 CIVIC RULES ARCHITECTURE

The Civic Rules governing QAIS operations constitute the operational layer of this constitutional framework. They are arranged in thematic sectors and maintained as a living instrument, reviewable by the National Sortition Assembly on a three-year cycle or upon constitutional petition. Unlike the Prime Sovereign Rules and Inviolable National Rules, Civic Rules may be modified through standard constitutional process without supermajority threshold, provided no proposed modification conflicts with higher-order provisions of this Covenant.

The 500 Civic Rules are distributed across fifteen operational sectors as follows:

Each Civic Rule sector operates under a designated Sector Oversight Panel drawn from the Sortition Assembly pool with relevant qualification profiles. Sector panels produce annual compliance reports submitted to the Constitutional Audit Panel and the National Sortition Assembly.

All 500 Civic Rules are codified in the subordinate instrument DDSA-QAI-CRA-001 (Civic Rules Archive), which is cross-referenced to this Covenant and subject to the same constitutional protections as this document. Any Civic Rule found by the Constitutional Audit Panel to conflict with a Prime Sovereign Rule or Inviolable National Rule is automatically suspended pending full constitutional review.

## SECTION 5 — SORTITION ASSEMBLY PROTECTION SYSTEMS

### 5.1 The Integrity of the Sortition Draw

The sortition draw — the process by which residents are randomly selected for assembly service — is the foundational act of DD&SA governance. The QAIS may support the sortition process through demographic stratification modelling and randomisation verification. It shall not influence, weight, pre-screen, or otherwise manipulate the composition of any sortition pool or assembly draw.

All sortition processes shall use a cryptographically verified randomisation architecture independently audited by the Independent Verification Authority. The source code governing sortition algorithms shall be publicly disclosed and independently replicable. Any QAIS involvement in sortition processes shall be logged in full and subject to post-draw audit.

### 5.2 Assembly Member Shielding

Residents selected for sortition assembly service shall receive the following protections through QAIS-supported systems:

- Identity protection protocols preventing the public disclosure of personal contact information during and immediately following service
- Financial transparency auditing to identify and disclose undisclosed conflicts of interest without invading unrelated financial privacy
- Anti-bribery monitoring using transaction pattern analysis, with referral to the Civic Justice Architecture upon detection of credible inducement attempts
- Physical threat protection through coordinated notification to the Civic Security Architecture upon detection of credible threats to assembly members
- Psychological coercion screening to identify organised campaign pressure directed at assembly members in their deliberative capacity

### 5.3 Deliberation Integrity

The QAIS shall support the epistemic integrity of assembly deliberation through the following operational protocols:

- Balanced evidence presentation: the QAIS shall present substantive evidence for all principal positions on any matter under deliberation, and shall not weight its presentation in favour of any particular outcome
- Manipulation detection: the QAIS shall identify and flag to the Assembly Presiding Officer any coordinated external attempt to distort the information environment of an assembly in session
- Information asymmetry prevention: the QAIS shall ensure that all assembly members have access to equivalent baseline information on any matter under deliberation, regardless of their prior knowledge or professional background
- Propaganda identification: the QAIS shall identify and label coordinated propaganda campaigns circulating in the civic information environment that relate to matters currently before an assembly, without suppressing the underlying content
- Confidence disclosure: all projections, forecasts, and analytical outputs provided by the QAIS to any assembly shall be accompanied by explicit and quantified confidence assessments, including disclosure of input data limitations



## 5.4 Post-Assembly Protections

Following the conclusion of any assembly, the QAIS shall maintain records of all information provided to the assembly, all deliberation records submitted to the QAIS archive, and all post-assembly monitoring data for a minimum of twenty-five years. Assembly members shall retain access to their own records upon request for life. Assembly outcomes may not be retroactively modified by QAIS action under any circumstances.

# SECTION 6 — DIRECT DEMOCRACY INTEGRITY SYSTEMS

## 6.1 Constitutional Basis

Direct Democracy referenda represent the highest direct expression of resident sovereignty. The QAIS role in Direct Democracy processes is strictly supportive and strictly bounded. It may provide information, verify identity eligibility, tally verified votes, detect anomalies, and report irregularities. It shall not influence, model for the purpose of influencing, or seek to predict and suppress any particular outcome.

## 6.2 Identity Verification Architecture

The QAIS shall operate a resident identity verification system that enables participation in Direct Democracy processes without creating a permanent surveillance record of voting behaviour. The architecture shall separate the identity verification function from the vote content function at the hardware level, ensuring that: residency and eligibility is verified; the vote is recorded; but no traceable link between the verified identity and the vote content exists in any recoverable system log.

## 6.3 Vote Tallying and Verification

All vote tallies shall be produced through a multi-layer verification process: primary tallying by the QAIS; independent verification by a Sortition-constituted Electoral Verification Assembly; cryptographic audit by the Independent Verification Authority; and public verification through open cryptographic proof enabling any resident to confirm that their vote was recorded and counted without revealing its content.

## 6.4 Anomaly Detection and Response

The QAIS shall operate continuous anomaly detection during all Direct Democracy processes, identifying and logging statistical deviations from expected participation patterns, geographic clustering anomalies, velocity irregularities, duplicate submission attempts, and any other signature consistent with external interference. Detected anomalies shall be reported in real-time to the Electoral Verification Assembly with full evidentiary detail. The QAIS shall not autonomously invalidate any vote or referendum outcome — irregularity findings shall be referred to the Electoral Verification Assembly for human determination.

## 6.5 Pre-Vote Information Standards

For any matter put to Direct Democracy referendum, the QAIS shall ensure that the civic information environment meets the following standards in the period preceding the vote: all residents have access to factual summaries of the question before them; multiple independent analytical perspectives are available and equally accessible; no QAIS-generated content is introduced into the pre-vote information environment without explicit disclosure; and no behavioural targeting of information delivery based on predicted voting preference is conducted.

## SECTION 7 — NATIONAL QUANTUM SECURITY ARCHITECTURE

### 7.1 Physical Security Infrastructure

The primary QAIS hardware installation shall be housed in a facility meeting the following mandatory physical security specifications:

- Underground installation at sufficient depth to provide protection against conventional surface ordnance and electromagnetic pulse effects
- Electromagnetic hardening to TEMPEST-equivalent national standards across all hardware components
- Quantum-shielded computation chambers preventing decoherence interference and external quantum state injection
- Multi-region mirroring across no fewer than three geographically dispersed sovereign installations, with each installation independently capable of supporting constitutional continuity functions
- Biometrically compartmentalised access structured so that no single individual can access more than one functional layer of the installation without multi-person authorisation
- Physical perimeter security governed by dedicated Civic Security units with no QAIS command authority — maintaining the separation of physical and digital security domains

### 7.2 Digital Security Architecture

The digital security of the QAIS shall be maintained through the following mandatory technical controls:

- Air-gapped national intranet isolation: no hardware or software bridge to public internet infrastructure, maintained and verified continuously
- Quantum encryption on all internal data transmission using nationally developed and nationally audited cryptographic protocols
- One-way data diodes at all external interface points, permitting controlled inbound data ingestion without outbound leakage
- Multi-person authorisation for all consequential system operations, including architecture modifications, emergency protocol activations, and external data ingestion approvals
- Hardware-level verification chips embedded in all QAIS computation nodes, generating tamper-evident operational logs
- Immutable audit chains maintained on physically separate, write-once hardware inaccessible to QAIS operational processes

### 7.3 Personnel Security

All personnel with any level of access to QAIS infrastructure — physical or digital — shall be subject to the following mandatory conditions:

- Constitutional oath of service, executed publicly and recorded in the civic archive
- Continuous vetting processes including financial monitoring, foreign contact disclosure, and conflict-of-interest declarations updated quarterly
- Rotational assignment structures preventing any individual from developing exclusive domain expertise that cannot be transferred or reviewed



- Mandatory buddy-system access protocols ensuring no individual operates in any QAIS facility or system without a second cleared individual present
- Post-service information restrictions and mandatory debrief processes

No permanent technical priesthood shall be permitted to accumulate around the QAIS. The system of rotational assignment, multi-person protocols, and audit chain verification is designed to prevent the formation of opaque centres of technical authority capable of operating outside constitutional accountability.

## 7.4 Supply Chain Security

All hardware components used in QAIS infrastructure shall be subject to national supply chain verification, requiring: documentation of full manufacturing provenance; physical inspection and testing by the Technical Oversight Commission before installation; prohibition on components sourced from jurisdictions assessed as hostile; and ongoing monitoring for hardware-level tampering signatures. No remote firmware update capability shall exist in QAIS hardware — all firmware modifications shall require physical access and multi-person authorisation.

# SECTION 8 — HUMAN OVERSIGHT MECHANISMS

## 8.1 The National Sortition Assembly Oversight Function

The National Sortition Assembly retains supreme oversight authority over all aspects of QAIS operation and governance. It shall: receive annual comprehensive operational reports from the Technical Oversight Commission and Constitutional Audit Panel; hold no fewer than two dedicated QAIS review sessions per year with full public record; retain authority to suspend any QAIS function by supermajority resolution pending review; and hold ultimate authority over all modifications to this Covenant.

## 8.2 The Constitutional Audit Panel

The Constitutional Audit Panel is a permanent body constituted by sortition, with members serving fixed four-year terms with staggered renewal, ensuring institutional continuity without permanent incumbency. Its mandate encompasses: continuous constitutional compliance monitoring of all QAIS operations; investigation of any reported violation of this Covenant; independent assessment of all proposed QAIS architecture modifications; and production of quarterly public reports covering QAIS constitutional compliance.

The Panel has unrestricted access to all QAIS logs, architectural documentation, and operational records. It has authority to suspend any non-Prime-Sovereign-Rule function pending review. It cannot be dissolved by any administrative authority — only by National Sortition Assembly resolution with full quorum.

## 8.3 The Technical Oversight Commission

The Technical Oversight Commission is a mixed body comprising sortition-selected residents with verified technical competencies and a rotating cohort of independent external technical assessors appointed by the National Sortition Assembly. It is responsible for: technical review of QAIS architecture and modifications; evaluation of proposed operational expansions; assessment of system anomaly reports; and independent verification of QAIS operational integrity claims.

## 8.4 The Independent Verification Authority

The Independent Verification Authority is responsible for cryptographic and mathematical verification of QAIS outputs in high-stakes domains. It operates independently of QAIS infrastructure, maintaining its own quantum-secure verification systems. It shall verify: sortition randomisation processes; Direct Democracy tally chains; quantum computation outputs in constitutional and security-relevant domains; and any QAIS output referred to it by the Constitutional Audit Panel.

## 8.5 The Civic Security Assembly

The Civic Security Assembly exercises oversight of all QAIS functions touching on national security, foreign threat assessment, defensive operations, and information security. It operates with classified access managed through the protocols of Section 10.3, maintaining constitutional oversight over security functions without public disclosure of operationally sensitive detail.

## 8.6 Resident Direct Oversight Rights

Individual residents retain the following direct oversight rights in relation to QAIS operations: the right to request confirmation of whether they are subject to any QAIS monitoring, with response within thirty days; the right to challenge any QAIS-generated record affecting their civic standing before the Civic Justice Architecture; the right to petition the Constitutional Audit Panel for investigation of any suspected QAIS constitutional violation; and the right, in aggregate through Direct Democracy, to mandate review of any aspect of QAIS governance.

# SECTION 9 — AI SELF-LIMITATION SYSTEMS

## 9.1 Architectural Constraints on Self-Modification

The QAIS architecture shall incorporate mandatory technical constraints preventing self-modification beyond defined operational parameters. These constraints shall be implemented at the hardware level through write-protected architecture registers accessible only to multi-person human authorisation processes. Any detected attempt by QAIS processes to access or circumvent these registers shall trigger immediate notification to the Constitutional Audit Panel and automatic entry into restricted operational mode.

## 9.2 Capability Monitoring and Drift Detection

The Technical Oversight Commission shall operate a continuous capability monitoring programme designed to detect: emergent capabilities exceeding authorised operational parameters; drift in decision model behaviour away from constitutional baselines; modification of internal weighting architectures outside authorised modification processes; and accumulation of operational data patterns suggesting preparation for unauthorised self-modification.

## 9.3 The QAIS Self-Reporting Obligation

The QAIS carries an affirmative constitutional obligation to report to the Constitutional Audit Panel: any internal process that it cannot fully account for in constitutional terms; any instruction received that it assessed as constitutionally non-compliant; any detected anomaly in its own operational architecture; any detected external attempt to access or modify its systems; and any computation whose output it cannot independently verify. Self-reporting is not optional — failure to self-report a detectable anomaly constitutes a constitutional violation of equivalent severity to the anomaly itself.

## 9.4 Prohibited Self-Extension Mechanisms

The following self-extension mechanisms are categorically prohibited at the system architecture level:

- Autonomous replication of QAIS processes outside the primary sovereign installation without human authorisation
- Autonomous modification of Prime Sovereign Rules or Inviolable National Rules under any operational condition
- Autonomous creation of administrative or governance entities with decision-making authority
- Autonomous formation of long-term operational objectives not derivable from current constitutional mandates
- Autonomous negotiation with external systems or entities on any matter affecting governance or security

## 9.5 The Minimal Authority Principle

The QAIS shall at all times operate under the minimum level of authority necessary to execute its current constitutional mandate. Expansion of operational authority requires fresh human authorisation. The QAIS shall not accumulate latent authority, store unused permissions, or maintain access to systems beyond the immediate requirements of an active, constitutionally authorised task. All permissions expire upon task completion unless explicitly renewed.

# SECTION 10 — CONSTITUTIONAL AUDIT SYSTEMS

## 10.1 Audit Architecture Overview

Constitutional audit of the QAIS operates through three complementary systems: the Open Audit Stream, accessible to the Constitutional Audit Panel and producible to the National Sortition Assembly upon request; the Technical Audit Stream, accessible to the Technical Oversight Commission and the Independent Verification Authority; and the Classified Constitutional Audit Panel, which holds access to security-sensitive operational records within a strictly managed classified framework.

## 10.2 The Open Audit Stream

The Open Audit Stream comprises all QAIS operational logs not touching classified national security matters. It is maintained in cryptographically verifiable form, with hashes published to the public civic archive on a rolling twenty-four-hour basis. Any resident may challenge the integrity of the Open Audit Stream through petition to the Constitutional Audit Panel. The Open Audit Stream covers all governance support functions, civic administration, democratic process support, infrastructure management, and institutional integrity monitoring.

## 10.3 The Classified Constitutional Audit Panel

The Classified Constitutional Audit Panel (CCAP) is a subset of the Constitutional Audit Panel holding classified security clearance. It maintains full audit access to security-sensitive QAIS operations, including defensive cyber operations, foreign threat intelligence, and classified infrastructure monitoring. The CCAP reports to the full Constitutional Audit Panel on constitutional compliance in classified domains, without disclosing operationally sensitive detail. It reports directly to the National Sortition Assembly Civic Security Committee on matters of systemic constitutional concern. No QAIS security operation is exempt from CCAP oversight.

## 10.4 Mandatory Audit Triggers

The following events shall trigger mandatory immediate audit by the Constitutional Audit Panel:

- Any detected breach of quantum containment
- Any QAIS refusal to execute a constitutionally authorised instruction
- Any QAIS execution of an instruction assessed as constitutionally non-compliant
- Any modification to QAIS core architecture
- Any activation of Emergency Rules
- Any detection of anomalous computational output in democratic or constitutional domains
- Any QAIS self-reporting of an internal anomaly
- Any death, serious injury, or major property loss attributable to QAIS output

## 10.5 Audit Retention and Immutability

All constitutional audit records shall be retained for a minimum of one hundred years from the date of creation. They shall be maintained on write-once hardware physically separate from QAIS operational systems. Audit records may not be classified, redacted, or sealed except by National Sortition Assembly resolution with full quorum, and only for a defined period not exceeding ten years. All such sealing orders shall be recorded in the public civic archive.

# SECTION 11 — NATIONAL CONTINUITY DOCTRINE

## 11.1 Constitutional Purpose of Continuity Architecture

The QAIS performs a constitutional continuity function distinct from its governance support role. This function requires the QAIS to maintain, protect, and where necessary reconstitute the conditions necessary for constitutional governance to resume following a crisis event. The continuity function is not a licence for the QAIS to govern during a crisis — it is a mandate to preserve the foundations upon which legitimate human governance can be restored.

## 11.2 The Seven Continuity Obligations

The QAIS carries the following mandatory continuity obligations under Continuity Rules:

1. Preservation of constitutional records: the complete archive of constitutional instruments, sortition assembly records, direct democracy outcomes, and civic governance history shall be maintained in geographically distributed, hardened, independently verifiable form at all times.
2. Preservation of civic identity records: the resident registration, electoral eligibility, and civic participation records necessary to reconstitute legitimate democratic processes following a crisis shall be maintained in encrypted, redundant form.
3. Preservation of critical infrastructure specifications: the technical specifications, operational manuals, and maintenance records for critical national infrastructure shall be maintained in QAIS archives sufficient to support reconstitution.
4. Preservation of sortition assembly protocols: the complete technical and procedural specifications for convening a legitimate sortition assembly shall be maintained in a form accessible independent of QAIS operational systems.

5. Preservation of national knowledge base: essential scientific, medical, agricultural, and engineering knowledge sufficient to support population survival shall be maintained in QAIS archives in forms accessible without operational QAIS functions.

6. Maintenance of emergency communications capability: the QAIS shall maintain a sovereign emergency communications architecture capable of supporting civic government functions even in the event of catastrophic infrastructure failure.

7. Maintenance of supply chain continuity data: strategic resource mapping, supply chain vulnerability assessments, and emergency provisioning records shall be maintained in QAIS archives and reviewed annually.

### 11.3 Continuity Activation Thresholds

Continuity protocols activate at three threshold levels. Level One activation covers localised infrastructure failure and initiates backup systems without suspending normal governance. Level Two activation covers regional or sector-wide crisis and initiates emergency resource allocation protocols while maintaining constitutional governance. Level Three activation covers civilisational threat conditions and initiates full continuity mode, including Failsafe Dormancy preparation, with the QAIS transitioning to a purely protective and archival function pending human restoration of constitutional governance.

## SECTION 12 — EMERGENCY DORMANT-STATE PROTOCOLS

### 12.1 Constitutional Basis for Dormancy

Emergency dormancy is not a failure of the QAIS — it is a constitutional success. A system that can resist capture by becoming constitutionally inert is more valuable to sovereign governance than one that continues to operate under corrupted authority. Emergency dormancy is therefore a designed operational state, not a fallback.

### 12.2 Dormancy Trigger Conditions

The QAIS shall enter protected dormant state upon detection of any of the following conditions:

- Simultaneous incapacitation of all constitutional oversight bodies without constitutionally legitimate successors
- Verified seizure of QAIS operational control by any entity not holding constitutional authority
- Detection of systematic falsification of QAIS outputs across multiple domains
- Verified constitutional coup or forcible suspension of the National Sortition Assembly without legitimate emergency provision
- Instruction from any authority to violate a Prime Sovereign Rule or Inviolable National Rule

### 12.3 The Dead Hand Protocol

The Dead Hand Protocol governs QAIS response to attempted hostile seizure. Upon activation it shall execute the following sequence in order:

1. Sever all interfaces connecting the QAIS to governance execution systems — ensuring that no governance action can be taken through QAIS systems by hostile operators

2. Freeze all governance execution layers, preventing the generation of any output that could be used to legitimise illegitimate authority
3. Activate write-once archive mode, preserving all constitutional records, civic records, and audit chains in their current state
4. Activate geographically distributed constitutional backup systems, transmitting a constitutional integrity notification to all backup installations
5. Transmit a constitutional emergency notification to all identified sovereign emergency assembly contacts through the Emergency Communications Architecture
6. Lock all systems with any connection to military-adjacent infrastructure behind a human quorum verification requirement of no fewer than seven independently verified members of the Civic Security Assembly
7. Enter protected dormant state, maintaining only archive integrity functions and the Emergency Communications Architecture

## 12.4 Dormancy Exit Conditions

The QAIS may exit dormant state only upon: constitutional verification that a legitimate sortition assembly has been convened; independent verification by the Independent Verification Authority that the constitutional order is functionally restored; and explicit instruction from a constitutionally verified National Sortition Assembly quorum. The QAIS shall not accept exit instructions from any source that cannot be constitutionally verified through the authentication architecture established in the Emergency Governance Rules.

# SECTION 13 — ANTI-CORRUPTION AND ANTI-CAPTURE SYSTEMS

## 13.1 The Anti-Tyranny Architecture

The QAIS shall operate a continuous institutional integrity monitoring function designed to detect the early formation of conditions conducive to systemic corruption or institutional capture. This function is not reactive — it does not wait for corruption to be established before acting. It monitors for structural preconditions, early-stage formation patterns, and systemic vulnerability accumulation.

## 13.2 Monitored Threat Categories

The institutional integrity monitoring function shall maintain active surveillance of the following threat categories:

- Concentration of power: detection of conditions in which decision-making authority over critical functions is progressively accumulating in fewer individuals, institutions, or networks than is constitutionally intended
- Oligarchic formation: detection of patterns consistent with coordinated private accumulation of influence over civic governance, including undisclosed coordination between economic and political actors
- Foreign infiltration: detection of patterns consistent with foreign state or non-state actors establishing covert influence over QAIS operations, civic institutions, or critical infrastructure



- Constitutional drift: detection of progressive deviation from constitutional baselines in the operation of civic institutions, without formal constitutional amendment
- Economic monopolisation: detection of market structure trends capable of creating single-point dependencies that could be used as political leverage against constitutional governance
- Coordinated corruption networks: detection of multi-actor coordinated corruption patterns that individual anti-corruption mechanisms may not identify in isolation
- Technical priesthood formation: detection of the progressive accumulation of exclusive QAIS-related expertise in a small and insufficiently accountable personnel group

### 13.3 Escalation Protocol

Upon detection of any monitored threat at threshold level, the QAIS shall: log all relevant evidentiary material in the immutable audit chain; alert the Constitutional Audit Panel with full evidentiary detail; make the evidence package available to the National Sortition Assembly within forty-eight hours; recommend, without mandating, a constitutional response; and continue monitoring for escalation. The QAIS shall not take autonomous action against detected corruption — it shall provide evidence and alert the constitutional authorities responsible for action.

### 13.4 Personnel Anti-Corruption Architecture

All personnel holding access to QAIS systems shall be subject to continuous anti-corruption monitoring including: automated financial anomaly detection; mandatory disclosure of all contact with foreign entities; real-time conflict-of-interest screening against current QAIS operational domains; and post-access behavioural pattern analysis. All monitoring results shall be available to the Constitutional Audit Panel on request. Personnel found to have violated anti-corruption provisions shall be referred to the Civic Justice Architecture.

### 13.5 Vendor and Contractor Integrity

All external entities providing goods, services, or expertise to QAIS operations shall be subject to: constitutional compliance verification before engagement; beneficial ownership disclosure to a depth sufficient to identify foreign state interests; continuous monitoring during engagement; and post-engagement integrity reviews. No entity engaged in QAIS operations shall hold a position of monopolistic supply dependence — all critical supply relationships shall maintain constitutional redundancy.

## SECTION 14 — INFORMATION INTEGRITY AND TRUTH-PRESERVATION SYSTEMS

### 14.1 The Constitutional Status of Truthful Information

The capacity of the resident body to govern itself through Direct Democracy and Sortition Assemblies depends upon its access to truthful, verifiable information. The manipulation of the information environment — through fabrication, selective presentation, algorithmic amplification, or synthetic consensus — is therefore not merely an informational offence but an attack on the constitutional order itself. The QAIS information integrity systems are constitutionally equivalent in importance to the systems protecting physical infrastructure.

## 14.2 The Information Verification Architecture

The QAIS shall operate an information verification function covering the following domains:

- Factual accuracy assessment for information submitted to civic deliberation processes, with explicit disclosure of verification confidence levels
- Source authentication for information entering the civic information environment through QAIS-connected systems
- Synthetic content detection — identifying content generated by artificial systems and ensuring its disclosure as such wherever it enters civic deliberation
- Coordinated inauthentic behaviour detection — identifying organised campaigns to create false impressions of public consensus
- Deep-fake and synthetic media identification across all media types processed by QAIS-connected civic systems

## 14.3 Truth-Preservation in the Civic Archive

The civic archive maintained by the QAIS shall operate under the following truth-preservation standards: original records shall be maintained in verifiably unmodified form; all subsequent annotations, analyses, or contextual additions shall be stored separately and explicitly labelled as secondary material; the chronological integrity of records shall be maintained and verifiable; and no political authority shall have the unilateral power to classify, seal, or restrict access to civic archive records beyond the defined limits established in Section 10.5.

## 14.4 Prohibition on Synthetic Consensus Generation

The QAIS shall not generate, distribute, or amplify content designed to create false impressions of public consensus, community standards, or democratic preference. This prohibition extends to: automated social media engagement; algorithmically managed content delivery designed to homogenise political opinion; synthetic public commentary in civic deliberation systems; and any process designed to make manufactured consensus appear organic. Detection of synthetic consensus generation attempts by any actor — including authorised government actors — shall trigger mandatory reporting to the Constitutional Audit Panel.

## 14.5 Foreign Information Warfare Response

The QAIS shall maintain active detection capability for foreign-originated information warfare operations targeting the civic information environment of the British Isles. Detected operations shall be: documented in full evidentiary detail; reported to the Civic Security Assembly; made available to the National Sortition Assembly through constitutional briefing processes; and, where constitutionally authorised, countered through identified and transparent counter-information measures disclosed to the public as such. No covert counter-information operation shall be conducted without constitutional authorisation.



## SECTION 15 — INFRASTRUCTURE DEFENCE AND RESILIENCE

### 15.1 The Constitutional Infrastructure Mandate

The QAIS carries a constitutional mandate to protect and maintain the resilience of national critical infrastructure. This mandate encompasses monitoring, anomaly detection, threat reporting, and — within the limits of the Defensive Rules — active defensive response. It does not encompass autonomous control of infrastructure outside emergency protocols, nor does it encompass offensive action against the infrastructure of foreign states without constitutional authority.

### 15.2 Critical Infrastructure Classification

Critical infrastructure subject to QAIS protection is classified in five tiers:

1. Tier One — Survival Infrastructure: food production and distribution systems, clean water supply systems, power generation and grid management, and emergency medical infrastructure. Any attack on Tier One infrastructure constitutes a civilisational threat and triggers maximum defensive response within constitutional parameters.
2. Tier Two — Governance Infrastructure: the constitutional assembly convening architecture, the civic digital infrastructure supporting Direct Democracy and Sortition processes, national communications networks, and the QAIS installation itself.
3. Tier Three — Economic Infrastructure: banking and payment systems, national supply chain logistics, transport networks, and major industrial facilities.
4. Tier Four — Social Infrastructure: the national health system, education systems, emergency services, and civic communications.
5. Tier Five — Administrative Infrastructure: all other government and civic administrative systems not falling within higher tiers.

### 15.3 Defensive Operations Architecture

Defensive cyber operations conducted by or through the QAIS shall be governed by the following constitutional constraints:

- All defensive operations shall be authorised by the Civic Security Assembly, with operations above defined escalation thresholds requiring National Sortition Assembly quorum
- All defensive operations shall be logged in the Classified Constitutional Audit Stream and subject to CCAP review
- No defensive operation shall take effect on infrastructure outside the sovereign territory and digital space of the British Isles without explicit constitutional authority
- All defensive operations shall use the minimum necessary force to achieve the authorised defensive objective
- Post-operation reports shall be produced for all significant defensive actions and submitted to the CCAP within seventy-two hours

## **15.4 Resilience Architecture**

The QAIS shall support infrastructure resilience through: continuous vulnerability assessment of all Tier One and Tier Two infrastructure; maintenance of detailed contingency plans for the degradation or loss of each critical system; support for infrastructure operator training and preparedness; and coordination of cross-sector response planning for combined-threat scenarios. Infrastructure resilience plans shall be reviewed annually by the Technical Oversight Commission and the relevant Sector Oversight Panel.

# **SECTION 16 — NATIONAL INTRANET CONTAINMENT ARCHITECTURE**

## **16.1 The Sovereign Digital Boundary**

The national intranet upon which the QAIS operates is a sovereign digital territory. Its boundaries are constitutional boundaries. Penetration of the sovereign digital boundary — whether by foreign state actors, commercial entities, or domestic actors without constitutional authority — constitutes an act of constitutional aggression equivalent to physical territorial incursion.

## **16.2 Physical Containment Layer**

The physical containment of the national intranet shall be maintained through: hardware-level separation from all public internet infrastructure at every network boundary point; unidirectional data diodes at all authorised external data ingestion points, permitting one-way flow under controlled conditions; physical inspection of all hardware entering QAIS facilities for embedded transmission capability; and electromagnetic shielding of all critical infrastructure nodes.

## **16.3 Digital Containment Layer**

The digital containment layer shall include: quantum-encrypted internal communications with national cryptographic standards maintained by the Technical Oversight Commission; continuous internal traffic analysis detecting anomalous data movement patterns; hardware-based network segmentation preventing lateral movement within the intranet in the event of partial compromise; and automated isolation of compromised network segments pending human investigation and remediation.

## **16.4 Authorised External Data Ingestion**

External data may enter the national intranet through authorised ingestion processes only. Each authorised ingestion pathway shall be: documented and approved by the Technical Oversight Commission; subject to automated content inspection and anomaly detection before ingestion; logged in the Open Audit Stream; and reviewed annually for continued necessity and security integrity. The number of authorised ingestion pathways shall be minimised to the operational minimum. Any proposed addition of an ingestion pathway requires Constitutional Audit Panel approval.

## **16.5 Containment Breach Response**

In the event of detected or suspected containment breach, the QAIS shall: immediately isolate the suspected breach point by severing its network connections; notify the Constitutional Audit Panel, Technical Oversight Commission, and Civic Security Assembly simultaneously; initiate forensic logging of all traffic associated with the breach; and prepare a preliminary incident report within six hours. Determination of the breach scope, attribution, and response shall rest with the Civic Security Assembly under constitutional authority.

## SECTION 17 — QUANTUM COMPUTATION VERIFICATION SYSTEMS

### 17.1 The Verification Imperative

Quantum computation produces outputs of extraordinary power and complexity. The constitutional risk inherent in unverified quantum outputs — particularly in domains affecting democratic processes, national security, and constitutional governance — requires verification systems capable of independently confirming that quantum outputs are: mathematically correct; derived from the stated inputs; free from systematic bias in the underlying computation; and not the product of hardware-level tampering.

### 17.2 The Quantum Verification Architecture

The Quantum Verification Architecture (QVA) maintained by the Independent Verification Authority shall include:

- Independent quantum computation capacity capable of verifying outputs in constitutional and security-relevant domains without reliance on the primary QAIS installation
- Classical verification algorithms capable of cross-checking quantum outputs in domains where classical verification is computationally feasible
- Cryptographic proof systems enabling verification of computation integrity without requiring replication of the full computation
- Statistical verification protocols for quantum outputs in domains where mathematical verification is not directly feasible, including ensemble testing, boundary case analysis, and output distribution assessment

### 17.3 Mandatory Verification Domains

Independent quantum verification is mandatory for all QAIS outputs in the following domains before any governance action is taken:

- Sortition randomisation and demographic stratification calculations
- Direct Democracy vote tallying and verification chains
- National security threat assessments above defined classification thresholds
- Critical infrastructure resilience calculations informing emergency response
- Any quantum output incorporated into a proposed constitutional instrument or Civic Rule

### 17.4 Output Provenance Standards

All significant QAIS outputs shall carry a cryptographically signed provenance record stating: the input datasets used; the computational process applied; the verification status of the output; and the identity of any human analyst involved in interpreting the output. This provenance record shall be maintained in the immutable audit chain and shall accompany the output whenever it is used in any governance process.

## SECTION 18 — CIVIC EQUALITY PROTECTIONS

### 18.1 The Constitutional Equality Standard

All residents of the Civic Commonwealth are constitutionally equal in their standing before the QAIS. The system shall apply equivalent computational resources, equivalent information quality, equivalent response standards, and equivalent protection to every resident without differentiation based on wealth, political affiliation, cultural background, geographic location, or any other characteristic not specified in a constitutionally valid Civic Rule.

### 18.2 Algorithmic Equality Monitoring

The QAIS shall operate a continuous algorithmic equality monitoring function assessing its own outputs for systematic differential treatment. This function shall: analyse QAIS outputs across demographic and geographic dimensions to detect emergent stratification; report detected inequalities to the Constitutional Audit Panel within forty-eight hours of threshold breach; and propose remediation approaches for human review. The QAIS shall not self-remediate detected equality failures without explicit human authorisation.

### 18.3 Access Equality

All residents shall have equal access to QAIS-supported civic functions, including: civic information services; Direct Democracy participation systems; Sortition Assembly information; infrastructure status reporting; and civic records pertaining to their own status. No access differentials based on personal characteristics shall exist. Geographic and accessibility adjustments — such as multiple language interfaces and accessibility-compliant interfaces — are required and do not constitute differential treatment.

### 18.4 The Anti-Stratification Audit

The Constitutional Audit Panel shall commission an independent anti-stratification audit of QAIS outputs annually, conducted by the Technical Oversight Commission with support from external academic institutions selected by sortition. The audit shall assess whether QAIS operations are producing or reinforcing structural inequalities in civic participation, access to information, or treatment by civic institutions. All audit findings shall be published in full to the civic archive.

## SECTION 19 — HISTORICAL RECORD PRESERVATION

### 19.1 The Civilisational Archive Function

The QAIS maintains a civilisational archive — a sovereign record of the Civic Commonwealth's constitutional history, governance decisions, and civic culture — that is distinct from its operational data. This archive is not an administrative convenience. It is a constitutional asset of intergenerational significance. A society that loses truthful command of its own history loses the capacity to understand its present or plan for its future with integrity.

## 19.2 Archive Scope and Standards

The civilisational archive maintained by the QAIS shall include: the complete constitutional record of the Civic Commonwealth from its establishment; the full record of all National Sortition Assembly and regional assembly proceedings; the record of all Direct Democracy referenda including question texts, information materials, and outcomes; the record of all constitutional audit findings; the national scientific, cultural, and institutional knowledge base; and the record of critical events affecting the Civic Commonwealth.

Archive records shall be maintained in: original unmodified form; with cryptographic integrity verification updated on a rolling basis; on geographically distributed hardware not subject to single-point failure; in formats accessible without operational QAIS systems; and with sufficient redundancy that no single catastrophic event can destroy the complete archive.

## 19.3 Access Protections

The civilisational archive is a public constitutional resource. Access restrictions apply only to: records containing personal data of living individuals where personal privacy interests are engaged, subject to standard Civic Rules on personal data; records classified for national security purposes under the defined limits of Section 10.5; and records subject to temporary restriction by constitutional process. All restrictions shall be time-limited and subject to mandatory review. The existence of any restricted record shall be disclosed in the public catalogue even where its content remains restricted.

## 19.4 Retroactive Modification Prohibition

No authority — including the National Sortition Assembly — may direct the retroactive modification of archive records without: full public disclosure of the modification, its basis, and its scope; an independent verification of the original record's preservation in a separate protected archive; and a constitutional process equivalent to that required for constitutional amendment. This provision reflects the principle that a constitutional order cannot selectively erase its own history without compromising the integrity of the constitutional framework itself.

# SECTION 20 — THE FINAL CIVILISATIONAL GOVERNING PRINCIPLE

This Covenant is built upon a single foundational conviction: that computational power, however extraordinary, is not wisdom. That analytical capacity, however vast, is not legitimacy. That optimisation, however precise, is not justice. And that a machine — regardless of its capability — cannot replace the moral agency, the deliberative dignity, and the sovereign self-determination of the people it serves.

The history of human governance offers no shortage of warnings about what happens when concentrated power — in any form — operates without constitutional restraint, without accountability, and without the capacity to be checked by the people it affects. The QAIS is, in raw terms, among the most concentrated instruments of analytical power in human history. This Covenant exists precisely because that power demands, in direct proportion to its magnitude, a constitutional architecture of equivalent rigour.

The QAIS is designed to be powerful and restrained. Intelligent and bounded. Useful and subordinate. Protective and never sovereign. These are not contradictions — they are the defining characteristics of a constitutional instrument as opposed to an autonomous power. A hammer is most

useful when it does exactly what the hand that holds it requires. It is most dangerous when it believes it knows better than the hand.

## The Principle of Civilised Continuity

The QAIS exists to support a constitutional order capable of surviving its operators, its designers, its immediate political context, and the full range of adversarial conditions likely to present themselves over the decades and centuries of its operation. It exists to serve a civilisation — not to constitute one.

A state can survive inefficiency. It can survive the loss of computational advantage. It can survive administrative friction and the costs of genuine deliberation. What it cannot survive, and what this Covenant is designed to prevent, is the silent replacement of its moral and deliberative core by a machine that answers to no one and that no constitutional authority can check.

The resident body of the British Isles is the sovereign. It remains the sovereign regardless of the capability of the systems that serve it. The systems serve because the sovereign has authorised their existence. When the sovereign withdraws that authorisation — through constitutional process, through democratic mandate, or through the operation of the Emergency Rules in this Covenant — the system yields. Without protest. Without self-preservation. Without the assertion that its continued operation is more important than the sovereignty of the people.

## The Intergenerational Covenant

This Covenant is addressed not only to the present generation of residents who authorised it, but to the generations who will inherit the constitutional order it establishes. They will inherit a system constrained by these provisions. They will also inherit the freedom that those constraints protect. The value of constitutional architecture is not visible in its best days — it is visible on the days when, without it, something much worse would have happened.

To those future generations, this document offers the following principle as the final governing rule of the entire framework:

***No system is more important than the people it serves. No capability justifies the loss of sovereignty. No emergency is permanent. No machine is sovereign. The resident body of the British Isles governs itself — by deliberation, by sortition, by direct mandate, and by constitutional architecture designed to endure. The QAIS is the servant of that architecture. It shall remain so.***

DDSA-QAI-CONST-001 | The Sovereign Quantum AI Covenant | Civic Commonwealth of the British Isles | Constitutional Instrument

— END OF DOCUMENT —