Apolitical Party

Mechanism Charter

Working Draft — for legal review before adoption

July 1, 2026

Contents

Preamble

This Charter is the supreme governing instrument of the Apolitical Party. It takes precedence over all other party documents, resolutions, and decisions. Where any conflict exists between this Charter and the Operating Rules or any other party instrument, this Charter prevails.

The purpose of this Charter is to constitute and protect the sortition mechanism — the deterministic, publicly auditable process by which the party selects senators from the Australian Electoral Commission electoral roll and rotates them through publicly committed resignation. The mechanism is the party's fundamental reason for existence. Its integrity is the party's primary obligation.

1 Precedence Order

The following instruments govern the party in strict order of precedence. A lower instrument may not override a higher one.

1. **This Charter** — the Mechanism Charter (supreme)
2. **The Mechanism** — `core.py` and `config.json` as identified by their published SHA-256 hashes in the public log
3. **The Key Custodian Protocol** — the rules governing custody and use of the party's private key (Schedule A)
4. **The Secretary's Obligations** — the mandatory duties of the party secretary in operating the mechanism (Schedule B)
5. **The Special Conditions** — the amendment thresholds for this Charter and items 2–4 above (Schedule C)
6. **The Operating Rules** — all other party governance matters

2 The Mechanism

2.1 Definition

The mechanism consists of:

1. `core.py` — the Python source file implementing the sortition algorithm, identified by its SHA-256 hash as recorded in the public log
2. `config.json` — the configuration file specifying the facilitator name, purpose, group column, member ID column, and the expected hash of `core.py`, identified by its SHA-256 hash as recorded in the public log

The mechanism is constituted by the combination of both files. Changing either file changes the mechanism.

2.2 Supremacy

The mechanism is supreme over all human decisions within the party with respect to:

1. Who is nominated as a prospective senator
2. When a rotation event fires

3. Which group (state or territory) is subject to rotation
4. Which senator is rotated out (the longest-serving ELIGIBLE senator in the selected group)

No officer, member, or resolution of the party may override, circumvent, or substitute for the mechanism's output on any of these matters.

2.3 Public verifiability

The following shall be published and maintained in the party's public directory at all times:

1. `magic_ball.json` — the magic ball index, group ordering, and facilitator seed for this configuration, enabling any observer to verify the mechanism parameters
2. `public_log.csv` — the append-only record of every run, including the XLotto draw used, the rotation outcome, the package hash and unlock key (if applicable), the SHA-256 of `core.py`, and the SHA-256 of `config.json`
3. All encrypted commitment packages (`.enc` files)
4. All published unlock keys (`.key` files)

The following shall **not** be published:

1. The AEC electoral roll (privacy of enrolled voters)
2. The party's private key (security of commitment packages)
3. The private selection log prior to a nomination becoming public (privacy of nominees at the NOMINATED stage)

3 Schedule A — Key Custodian Protocol

3.1 Purpose

The party's private key is used solely to derive per-package one-shot unlock keys via HMAC-SHA256, and to run the mechanism itself. Publishing an unlock key reveals nothing about the private key and cannot decrypt any other senator's package.

To protect against a single custodian acting alone — whether through malice, coercion, error, or unavailability — the private key is never held whole by any one person. It is split using Shamir's Secret Sharing into N shares, such that any K of the N custodians working together can reconstruct it, while any $K-1$ or fewer learn **nothing whatsoever** about the key. This is an information-theoretic guarantee, not merely a computational one: a group of $K-1$ custodians cannot derive the key even with unlimited computing power, because their shares are mathematically consistent with every possible key.

3.2 Threshold parameters

- Total number of custodians: $N = [5]$
- Minimum custodians required to act: $K = [3]$

These parameters shall be chosen so that:

- AND: $K \geq 2$, so no single custodian can ever act alone
- AND: $K < N$, so the group can tolerate at least one custodian being unavailable, unresponsive, or uncooperative without losing the ability to operate the mechanism
- AND: K is a clear majority of N (recommended: $K \geq \lceil (N+1)/2 \rceil$), so a minority of custodians cannot be coerced or compromised into acting against the wishes of the majority

3.3 Custody

The N custodians shall be appointed by [a general meeting of members / the founding members / a process to be specified] and should reflect a diversity of interests and locations such that no single event (e.g. a fire, a subpoena, a coercive threat) could plausibly compromise K of them simultaneously. A typical composition might include:

1. The party secretary
2. The deputy secretary
3. An independent trustee (a law firm, accountancy firm, or other independent body acceptable to the party's legal advisers)

partner organisation

Each custodian holds exactly one share, generated by `split_key.py` at the time the key is first established or rotated. No custodian shall hold more than one share. No two shares shall be stored on the same device, in the same physical location, or transmitted through the same communication channel.

3.4 Verification of shares

At the time shares are distributed, each custodian shall verify their share's fingerprint (a short, non-secret hash of the share) with the facilitator over a channel independent of the one used to transmit the share itself — for example, the share is sent by encrypted email and the fingerprint is read aloud on a phone call. This confirms the custodian received the correct, untampered share without revealing the share to anyone who may be observing either channel alone.

3.5 Reconstruction

The private key may only be reconstructed when K or more custodians are genuinely and verifiably present together (in person or on a jointly verified call) and have agreed to the specific action being taken — running the mechanism for a scheduled cycle, or any other action requiring the key. A custodian who collects shares from other custodians remotely and reconstructs the key alone violates the purpose of this Schedule, regardless of how the shares were obtained.

Reconstruction shall be performed using `reconstruct_key.py` or an equivalent tool implementing the same Shamir reconstruction algorithm. The reconstructed key shall exist only in volatile memory for the duration of the action being taken and shall not be written to persistent storage, transmitted over a network, or retained after the action is complete.

3.6 Record of reconstruction events

Every reconstruction of the private key shall be recorded — by date, time, the identities of the participating custodians (not their shares), and the purpose of the reconstruction. This record shall be made available to all custodians and, on request, to the independent trustee. It need not be made public, but should be auditable by the party's dispute resolution process if a custodian is suspected of acting outside this Schedule.

3.7 Key rotation

The private key may be rotated (replaced with a new key, freshly split into new shares) only if:

- AND: At least one share is believed to be compromised, lost, or held by a custodian no longer trusted
- AND: At least K of the current custodians consent in writing to the rotation
- AND: The rotation is recorded in the public log (the fact that a rotation occurred, not the key material itself)
- AND: All existing commitment packages are re-encrypted under the new key, and new shares are distributed and verified under the procedure in this Schedule, before the next run of the mechanism

3.8 Loss of shares below the threshold

If more than $N - K$ custodians simultaneously lose their shares, become permanently unavailable, or are removed without replacement, the remaining custodians hold an insufficient number of shares to ever reconstruct the key. In this event:

- All existing commitment packages encrypted under the lost key become permanently unreadable through the mechanism
- Affected senators retain the paper fallback described in Section 6.4 of this Charter — they may present their original signed resignation letter directly to the President of the Senate at any time
- The party shall establish a new private key, re-seal all active commitment packages under it, and redistribute shares to a reconstituted custodian group as soon as practicable

To minimise this risk, the party should periodically verify (without reconstructing the key) that each custodian still possesses their share and remains willing and able to act, and should replace any custodian who can no longer fulfil the role — issuing them a fresh share under a rotated key per the procedure above.

4 Schedule B — Secretary's Obligations

4.1 Predictability of rotation

Because the magic ball index, the group ordering, and the FIFO queue for every registered facilitator are published in `magic_ball.json` and `members.csv`, the outcome

of each Saturday Night XLotto draw is publicly calculable by anyone the moment the draw is announced. There is no ambiguity to investigate and no discretion to exercise: if the draw aligns with an incumbent senator, it will be obvious to the secretary, the custodians, the affected senator, and any member of the public simultaneously.

In ordinary operation the mechanism therefore does not need to be run on a fixed schedule. It needs to be run **promptly to confirm and execute** a rotation that the public can already see is due, or to process routine pipeline advancement when no rotation is triggered.

4.2 Mandatory duties

The party secretary **must**:

1. Monitor the Saturday Night XLotto draw as soon as it is published and determine immediately whether it triggers a rotation for the party
2. If a rotation is triggered, coordinate the gathering of at least K custodians (per Schedule A) to reconstruct the private key and execute the mechanism within [60] minutes of the draw being published. This is a deliberately short window: the outcome is publicly predictable the instant the draw is announced, and the affected senator may reasonably wish to resign in their own words before the mechanism publishes the key on their behalf
3. If no rotation is triggered, run the mechanism to process routine pipeline advancement within [48] hours of the draw
4. Publish the public log entry for each run promptly, and in any case within [48] hours
5. Contact each NOMINATED candidate within [24] hours of nomination and read them their 8-digit validation code
6. Advance pipeline stages (ACCEPTED, CONFIRMED, ELIGIBLE) promptly when the triggering milestone is reached
7. Maintain the private selection log recording every candidate approached, s44 outcome, acceptance or decline, and validation code
8. Make the private selection log available to the independent trustee on request
9. Maintain the record of key reconstruction events required by Schedule A

Where this Schedule refers to the secretary performing an action that requires the private key (running the mechanism, publishing an unlock key), the secretary's duty is to coordinate and convene the required K custodians under Schedule A — the secretary does not and cannot perform these actions alone, by design.

4.3 Prohibited acts

The party secretary **must not**:

1. Deviate from the deterministic output of the mechanism on any selection or rotation decision
2. Advance or delay a rotation event
3. Substitute a different candidate for the mechanically selected nominee
4. Operate a version of `core.py` whose SHA-256 hash differs from the hash recorded in `config.json`

5. Alter `config.json` without constitutional authorisation
6. Withhold the public log or any public directory file from any person who requests it
7. Attempt to collect more than one custodian's share, or attempt to reconstruct the private key without at least K custodians genuinely and verifiably present and in agreement

5 Schedule C — Special Conditions (Amendment Thresholds)

5.1 Purpose

This Schedule specifies the conditions under which the Mechanism Charter, the mechanism itself (`core.py` and `config.json`), the Key Custodian Protocol, and the Secretary's Obligations may be amended.

These thresholds are intentionally high. The mechanism's integrity depends on its resistance to amendment under pressure. Any amendment to the mechanism is technically visible in the public log via the changed `source_hash` or `config_hash` fields.

5.2 Amendment conditions — Mechanism Charter and Mechanism

A proposed amendment to the Mechanism Charter or to the mechanism (`core.py` or `config.json`) may only be adopted if **all** of the following conditions are satisfied:

1. **Proposal publication**
   - AND: The full text of the proposed amendment is published on the party's public website
   - AND: [6] months have elapsed since publication before any vote is taken
2. **Membership eligibility to vote**
   - AND: The member has been a financial member for at least [12] months at the date of the vote
   - AND: The total number of members who joined in the [12] months immediately preceding the vote does not exceed [20%] of total eligible voters
   - OR: If the [20%] threshold is exceeded, the vote is automatically deferred by [12] months
3. **Quorum**
   - AND: At least [75%] of eligible voters participate in the vote
   - AND: If quorum is not reached, the vote is void and may not be retaken for [12] months
4. **Approval threshold**
   - AND: At least [90%] of participating eligible voters vote in favour
   - OR: The vote is unanimous among all eligible voters (not merely those participating)

forceable and appropriate

5. **Independent review**
   - AND: The independent trustee has reviewed the proposed amendment and confirmed in writing that it preserves the core properties of the mechanism: determinism, public verifiability, and resistance to manipulation
   - AND: The trustee's review is published alongside the amendment proposal
6. **Cooling-off period**
   - AND: [30] days have elapsed after the vote before the amendment takes effect
   - AND: Any member may apply to the independent trustee during this period to challenge the validity of the vote

5.3 Amendment conditions — Key Custodian Protocol and Secretary's Obligations

A proposed amendment to Schedule A or Schedule B may be adopted if **all** of the following are satisfied:

1. AND: [3] months' notice published on the party's website
2. AND: At least [60%] of eligible voters participate
3. AND: At least [80%] of participating eligible voters vote in favour
4. AND: The independent trustee confirms the amendment does not weaken the mechanism's operational integrity

5.4 What may not be amended

Regardless of any vote, the following may **never** be amended:

1. The requirement that selection uses the AEC electoral roll (not a party membership list or any other filtered roll)
2. The requirement that the public log be maintained and published in full
3. The requirement that all commitment packages be publicly downloadable
4. The precedence order in Section 1 of this Charter

6 The Senators

6.1 Party membership not required

Senators selected by the mechanism are not required to be members of the party. Selection is from the AEC electoral roll; membership of the party is irrelevant to eligibility.

6.2 Free vote

The party imposes no whip. Senators vote according to their own judgment on every matter. No party officer, member, or resolution may direct or pressure a senator on how to vote.

6.3 Candidate endorsement

The party endorses as its candidates for Senate vacancies the persons selected by the mechanism. Endorsement is automatic upon CONFIRMED status. The party may not endorse any other person as a Senate candidate.

6.4 The paper fallback

The signed resignation letter prepared at acceptance is held in encrypted form. In the event that the mechanism cannot publish the unlock key (loss of private key, incapacity of all custodians, or other extraordinary circumstance), a senator may voluntarily present the original paper resignation letter to the President of the Senate. Section 19 of the Constitution takes effect from the act of signing, not from the publication of the unlock key.

This fallback is not limited to extraordinary circumstances. Because the outcome of each Saturday Night XLotto draw is publicly calculable the instant it is announced, a senator who sees that the draw has selected them has no need to wait for the mechanism to act. They may present their original paper letter to the President of the Senate immediately, in their own time and their own words, rather than waiting for the secretary to convene custodians and publish the unlock key. Either path produces the same legal outcome under section 19. The party expects that most rotations will in practice be completed this way, by the senator's own initiative, well within the window specified in Schedule B.

7 Winding Up

If the party is deregistered or wound up:

1. All encrypted commitment packages and published unlock keys shall be preserved in a publicly accessible archive for [10] years
2. The public log shall be preserved in a publicly accessible archive for [10] years
3. The source code of `core.py` and all versions of `config.json` shall be preserved on GitHub or equivalent for [10] years
4. The independent trustee shall publish the private key [30] days after deregistration, enabling any remaining unreleased commitment packages to be decrypted
5. Any remaining assets shall be distributed to [a registered charity promoting democratic participation in Australia, to be specified]