# ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)

# NON-DISCLOSURE AGREEMENT (NDA) POLICY

**PART I**

**PREAMBLE, CONTEXT, OBJECTIVES, PRINCIPLES, AND LEGAL BASIS**

## 1. Title, Citation, and Commencement

1.1. This instrument shall be cited as the **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC) All-Inclusive Non-Disclosure Agreement (NDA) Policy**, hereinafter referred to as *"the Policy."*

1.2. This Policy shall come into operation upon adoption and ratification by the **National Executive Committee (NEC)** of AAAIC and shall remain in force until duly amended or repealed in accordance with the prescribed procedures.

1.3. The provisions of this Policy are binding upon all members, office bearers, employees, volunteers, partners, service providers, and any person or entity engaged by AAAIC in any official or representative capacity.

1.4. This Policy shall be read and interpreted in conjunction with the **Constitution of the ARISE AFRIKA ARISE INDEPENDENT CONGRESS**, the **Code of Conduct and Ethics**, and all other policies or instruments adopted by the organisation.

## 2. Preamble and Policy Intent

2.1. **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC),** as a people-centered political organisation committed to integrity, transparency, and accountability, recognises the critical importance of confidentiality and the protection of sensitive information in ensuring the credibility and operational integrity of the movement.

2.2. In pursuit of its constitutional and strategic objectives, the AAAIC routinely generates, receives, stores, and processes information of a sensitive, strategic, political, financial, or personal nature. Such information, if improperly disclosed, may endanger the safety of members, compromise the organisation's operations, or cause irreparable reputational harm.

2.3. This Policy is therefore established to provide a **uniform, enforceable, and comprehensive framework** governing the protection, classification, handling, and disclosure of information across all tiers of the organisation.

2.4. The intent of this Policy is to:

- Protect all confidential, classified, and privileged information belonging to AAAIC;
- Prevent unauthorised disclosure or misuse of information by any person affiliated with the organisation;
- Promote disciplined communication and accountability across all structures; and
- Uphold the principles of integrity, loyalty, and confidentiality that underpin the values of AAAIC.

2.5. The Policy further seeks to cultivate a culture of responsibility and trust, ensuring that all individuals entrusted with information understand the **ethical, legal, and disciplinary implications** of their conduct in relation to confidentiality.

## 3. Policy Objectives

3.1. The objectives of this Policy are to:

(a) Define and institutionalise confidentiality protocols applicable to all organisational levels and committees;
(b) Establish the scope and legal basis for non-disclosure obligations across all internal and external relationships;
(c) Prescribe procedures for the signing, management, and enforcement of Non-Disclosure Agreements (NDAs);

(d) Provide clarity on the classification, storage, transmission, and disposal of confidential information;
(e) Define the responsibilities of members, office bearers, and contracted service providers regarding confidential data;
(f) Ensure compliance with national laws, including the **Protection of Personal Information Act (POPIA)**, the **Political Party Funding Act**, and related legislation
(g) Set out disciplinary and legal consequences for breach of confidentiality; and
(h) Strengthen AAAIC's internal governance, security, and public trust through a coherent confidentiality management framework.

## 4. Guiding Principles

4.1. The implementation of this Policy shall be guided by the following core principles:

(a) **Confidentiality:** Information designated as confidential shall be strictly protected and disclosed only on a need-to-know basis or by lawful authority.

(b) **Accountability:** Every individual with access to AAAIC information bears a direct duty of care and accountability.

(c) **Integrity:** All communication and information-handling must align with the ethical and moral values of the movement.

(d) **Lawfulness:** All practices under this Policy shall comply with the Constitution of the Republic of South Africa, relevant statutes, and AAAIC's internal regulatory instruments.

(e) **Transparency in Classification:** Information shall be classified according to established criteria, ensuring clarity between what is confidential and what may be publicly disclosed.

(f) **Proportionality:** The level of protection accorded to information shall be proportionate to its sensitivity and potential impact if disclosed.

(g) **Equity and Inclusivity:** The Policy applies uniformly and fairly to all tiers, ensuring no discriminatory enforcement or selective protection.

(h) **Institutional Loyalty:** All members and affiliates owe a duty of loyalty to AAAIC, superseding personal, factional, or external interests where confidentiality is concerned.

## 5. Legal and Constitutional Framework

5.1. This Policy derives its authority from and shall be interpreted in harmony with the following legal and regulatory instruments:

(a) **The Constitution of the Republic of South Africa, 1996**, particularly sections guaranteeing the right to privacy, the protection of personal information, and lawful administrative action;

(b) **The Protection of Personal Information Act (Act No. 4 of 2013)** — governing the lawful collection, processing, and safeguarding of personal and organisational data;

(c) **The Political Party Funding Act (Act No. 6 of 2018)** — providing for transparency in political party financing, within the limits of confidentiality and lawful disclosure;

(d) **The Promotion of Access to Information Act (Act No. 2 of 2000)** — which balances public access to information with the right to protect legitimate confidential records;

(e) **The Cybercrimes Act (Act No. 19 of 2020)** — regulating offences involving unlawful access, interception, or disclosure of data;

(f) **The Labour Relations Act (Act No. 66 of 1995)** — insofar as it governs confidentiality clauses within employment and contractual contexts; and

(g) **Common law principles** relating to the protection of trade secrets, fiduciary duties, and contractual confidentiality.

5.2. Within AAAIC, this Policy complements and reinforces:

- The **AAAIC Constitution and Code of Conduct**;
- The **Ethics and Integrity Policy**;
- The **ICT, Media, and Communications Policy**;
- The **Human Resource and Disciplinary Policy**; and
- The **Records Management and Data Protection Policy** (where applicable).

## 6. Application and Scope

6.1. This Policy applies to all tiers, organs, and associated entities of the AAAIC, including but not limited to:

(a) The **National Executive Committee (NEC)** and its subcommittees;
(b) The **National Working Committee (NWC)**;
(c) **Provincial, Regional, and Branch Executives**;
(d) The **Youth, Women, Veterans, and Sectoral Leagues**;
(e) **Task Teams, Commissions, and Ad Hoc Committees**;
(f) **Employees, interns, and volunteers**;
(g) **Consultants, advisors, contractors, and service providers**; and
(h) Any external party granted access to AAAIC information or property.

6.2. All members and officials are required, upon appointment, election, employment, or engagement, to sign a **Non-Disclosure Agreement** (Annexure A) acknowledging their obligations under this Policy.

6.3. The confidentiality obligations herein extend **beyond the duration of membership or employment**, and shall continue indefinitely in respect of information obtained during service to AAAIC.

## 7. Relationship to Other Instruments

7.1. This Policy forms an integral component of AAAIC's internal regulatory framework and shall be read in harmony with the organisation's founding documents.

7.2. Where any inconsistency arises between this Policy and another AAAIC policy, the interpretation that affords the **greatest degree of confidentiality protection** shall prevail.

7.3. Nothing in this Policy shall be construed to limit the rights of members under the AAAIC Constitution, provided that such rights are exercised without compromising confidentiality or breaching fiduciary obligations.

7.4. The NEC shall retain final interpretive authority over this Policy and may issue **Directives, Practice Notes, or Circulars** to ensure uniform understanding and application.

## 8. Policy Commitment Statement

8.1. AAAIC commits itself to maintaining the highest standards of confidentiality, discretion, and security in all its affairs.

8.2. The organisation affirms that information is a **strategic asset**, and its misuse constitutes not only an ethical violation but a potential act of sabotage or misconduct.

8.3. Through this Policy, AAAIC declares zero tolerance for unauthorised disclosures, leaks, or misappropriation of information, and commits to enforcing disciplinary, civil, or criminal measures where necessary.

8.4. All office bearers, members, and associates are required to internalise the principle that "**Confidentiality is a Covenant of Trust**," fundamental to the integrity and survival of the organisation.

## 9. Authority and Custodianship

9.1. The **Secretary-General** shall serve as the custodian of this Policy and is responsible for its dissemination, enforcement, and periodic review.

9.2. Each organisational level (provincial, regional, and branch) shall designate a **Confidentiality Officer** responsible for:

- Overseeing the signing and filing of NDAs;
- Managing secure document storage;
- Reporting potential breaches; and
- Coordinating training and compliance initiatives.

9.3. The NEC shall oversee policy compliance, receive periodic reports from the Secretary-General, and institute disciplinary or corrective measures as required.

**10. Commencement, Enforcement, and Review**

10.1. This Policy takes effect upon formal adoption by resolution of the **National Executive Committee (NEC)**.

10.2. Enforcement shall be immediate, with transitional arrangements for members or committees yet to sign NDAs.

10.3. The Policy shall be subject to review every **three (3) years** or sooner if necessitated by legislative amendments, technological developments, or organisational restructuring.

10.4. Amendments shall be tabled before the NEC for consideration and adoption by simple majority resolution.

## PART II

## DEFINITIONS AND INTERPRETATION

**1. Purpose of this Part**

1.1. The purpose of this Part is to provide a uniform and authoritative interpretation of all key terms and concepts used in this Policy, thereby ensuring consistency, predictability, and legal certainty in its application.

1.2. Unless otherwise stated, all words and expressions used in this Policy shall bear the ordinary meaning assigned to them in the context of South African law and the internal constitutional framework of **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)**.

## 2. Definitions

For the purpose of this Policy, unless the context indicates otherwise, the following terms shall bear the meanings assigned to them below:

**2.1. "AAAIC"**
Means **ARISE AFRIKA ARISE INDEPENDENT CONGRESS**, a registered political organisation established under South African law, together with all its organs, leagues, committees, substructures, and affiliated entities, as recognised in its Constitution.

**2.2. "Affiliate"**
Means any natural or juristic person who, though not a formal member, has a recognised association, partnership, or working relationship with AAAIC and is bound by the obligations of confidentiality under this Policy.

**2.3. "Agreement" or "NDA"**
Refers to the **Non-Disclosure Agreement**—a legally binding instrument signed by any person to whom this Policy applies, acknowledging the duty to protect and not disclose confidential information belonging to AAAIC.

**2.4. "Breach"**
Means any unauthorised disclosure, misuse, publication, loss, destruction, or alteration of confidential information, whether intentional, negligent, or inadvertent, and whether committed by act or omission.

**2.5. "Committee"**
Includes any permanent, ad hoc, or special committee, commission, or working group established under the authority of the NEC, NWC, or any subordinate structure of AAAIC.

**2.6. “Confidential Information”**

Means any information, in whatever form or medium, whether written, oral, digital, or recorded, that is not publicly available and is designated or reasonably understood to be confidential by virtue of its content, context, or purpose.

Without limitation, *Confidential Information* includes:

- Internal correspondence, reports, and memoranda;
- Minutes of meetings and deliberations of committees;
- Political strategies, campaign plans, or negotiation documents;
- Membership data, records, and contact lists;
- Financial records, budgets, and donor information;
- Information relating to disciplinary or investigative processes;
- Information concerning pending litigation, policy drafts, or electoral operations;
- Passwords, digital credentials, or system access codes; and
- Any other information expressly designated as “confidential” by authorised AAAIC officials.

**2.7. “Confidentiality Officer”**

Means the designated official at national, provincial, regional, or branch level responsible for implementing this Policy, ensuring NDA compliance, managing classified records, and reporting breaches to the Secretary-General.

**2.8. “Contractor” or “Service Provider”**

Refers to any person, company, consultant, or entity engaged by AAAIC under a contract, service-level agreement, or memorandum of understanding, who gains access to confidential information in the course of rendering services.

**2.9. “Data Subject”**

Has the meaning ascribed to it under the **Protection of Personal Information Act (POPIA)** and refers to any identifiable living natural person or juristic person about whom AAAIC holds personal or confidential information.

**2.10. “Disclosure”**

Means any form of communication, publication, transmission, dissemination, sharing, or making known of confidential information to any person or entity not authorised to receive such information, regardless of the means used (oral, written, electronic, or otherwise).

**2.11. “Document”**

Includes any record, file, memorandum, correspondence, report, or communication, whether in printed, handwritten, audio, video, or digital form, and whether stored physically or electronically.

**2.12. “Donor Information”**

Means any data, record, or identity of a person or entity providing financial or material support to AAAIC, whether disclosed voluntarily or under statutory reporting obligations, and protected within the limits of applicable law.

**2.13. “Electronic Communication”**

Refers to any communication transmitted or received through digital or electronic means, including but not limited to email, instant messaging, online conferencing, or data storage systems.

**2.14. “Fiduciary Duty”**

Means the duty of trust, loyalty, and good faith owed by all AAAIC members, officials, and affiliates to act in the best interests of the organisation and to refrain from using confidential information for personal or external gain.

**2.15. “Information Classification”**

Refers to the process of designating information into categories according to sensitivity, strategic importance, or potential harm if disclosed, including categories such as *Top Secret, Restricted, Internal Use, or Public*.

**2.16. “Insider”**

Means any individual who has or previously had authorised access to confidential information by virtue of position, office, or engagement with AAAIC, and whose obligations under this Policy persist beyond the termination of such relationship.

**2.17. “Leak”**

Means any unauthorised release of confidential information into the public domain, media, or social platforms, whether through direct disclosure, negligence, or deliberate manipulation.

**2.18. “Member”**

Means any person duly registered as a member of AAAIC under its Constitution and subject to all obligations, rights, and disciplinary processes prescribed therein.

**2.19. “Misuse of Information”**

Means any unauthorised use, alteration, or manipulation of confidential information for personal, factional, or third-party advantage, contrary to the objectives of AAAIC.

**2.20. “National Executive Committee (NEC)”**

Refers to the highest decision-making body of AAAIC between National Conferences, responsible for the adoption, interpretation, and enforcement of this Policy.

**2.21 “Need-to-Know Principle”**

Means the standard by which access to confidential information shall be limited strictly to those individuals whose functions, responsibilities, or mandates require such access.

**2.22. “Personal Information”**

Shall bear the meaning ascribed to it in section 1 of the **Protection of Personal Information Act**, and includes any information relating to an identifiable person, including but not limited to names, identification numbers, contact details, opinions, and other personal data processed by AAAIC.

**2.23. “Policy”**

Means this **All-Inclusive Non-Disclosure Agreement Policy** of **ARISE AFRIKA ARISE INDEPENDENT CONGRESS**, as adopted and amended from time to time.

**2.24. “Political Information”**

Refers to any internal strategy, campaign material, negotiation document, research, or deliberation undertaken by AAAIC for political, electoral, or organisational purposes, and classified as confidential by its nature.

**2.25. “Record”**

Means any recorded information, regardless of form or medium, which AAAIC has created, received, or retains in connection with its functions and activities.

**2.26. “Restricted Information”**

Means information which, though not classified as top secret, is subject to limited internal distribution and requires prior authorisation before being shared outside the defined structure.

**2.27. “Secretary-General”**

Means the principal administrative officer of AAAIC, vested with custodianship and oversight of all policies, including this Policy, and responsible for issuing directives relating to confidentiality and enforcement.

**2.28. “Sensitive Meeting”**

Means any meeting, caucus, conference, or session of AAAIC where matters of political, disciplinary, financial, or strategic importance are discussed and for which access, documentation, or recording is strictly controlled.

**2.29. “Third Party”**

Means any person or entity other than AAAIC or its members, including external organisations, government departments, or individuals, who may receive information under limited and authorised circumstances.

**2.30. “Whistleblower”**

Means a person who, acting in good faith and in the public or organisational interest, discloses information concerning unlawful, unethical, or irregular conduct within AAAIC through prescribed internal or legal channels, without malice or intent to harm.

**2.31. “Work Product”**

Refers to any document, draft, concept, design, communication, or output created in the course of fulfilling duties or functions within AAAIC, which remains the intellectual property of the organisation and subject to this Policy.

**2.32. “Unauthorised Person”**

Means any individual or entity who does not possess legitimate authority or clearance to access, handle, or disseminate confidential information of AAAIC.

**2.33. “Security Clearance”**

Means the formal authorisation or level of trust assigned to a person permitting access to specific categories of information, determined by the Confidentiality Officer or NEC directive.

**2.34. “Organisational Tier”**

Means any structural level within AAAIC—namely, national, provincial, regional, branch, or affiliated league—each of which is bound by the same obligations of confidentiality as prescribed in this Policy.

**2.35. “Internal Communication”**

Refers to any written, oral, or electronic exchange occurring within AAAIC structures and not intended for public dissemination.

**2.36. “Policy Breach Report”**

Means the formal document submitted to the Confidentiality Officer or Secretary-General in the event of a suspected or confirmed breach, in the format prescribed under Annexure B.

**2.37. “Official Capacity”**

Means the exercise of duties, functions, or roles on behalf of AAAIC, whether elected, appointed, or contracted, and includes all acts performed under such authority.

**2.38. “Retention Period”**

Means the prescribed duration for which confidential information shall be stored, retained, or archived before authorised destruction or declassification.

**2.39. “Disciplinary Action”**

Means any formal measure, including suspension, expulsion, reprimand, or termination, taken against a member or official found guilty of breaching this Policy or the associated NDA.

**2.40. “Policy Custodian”**

Means the office or person designated by the NEC—ordinarily the Secretary-General—to maintain, interpret, and oversee the consistent application of this Policy throughout AAAIC.

## 3. Interpretation Rules

3.1. The masculine includes the feminine, and vice versa; the singular includes the plural, and vice versa.

3.2. Headings and subheadings are for convenience only and shall not affect the interpretation of the text.

3.3. Any reference to a statute includes any amendment or re-enactment thereof.

3.4. Any reference to AAAIC organs or positions shall include their legitimate successors or equivalents established under restructured governance arrangements.

3.5. In the event of ambiguity or conflict, the interpretation most consistent with the principles of confidentiality, loyalty, and organisational integrity shall prevail.

3.6. Examples and illustrative clauses are included for explanatory purposes and do not limit or restrict the general application of this Policy.

## 4. Acronyms and Abbreviations

| Acronym | Full Meaning |
|---|---|
| AAAIC | **ARISE AFRIKA ARISE INDEPENDENT CONGRESS** |
| NEC | National Executive Committee |
| NWC | National Working Committee |
| NDA | Non-Disclosure Agreement |
| POPIA | Protection of Personal Information Act |
| PAIA | Promotion of Access to Information Act |
| ICT | Information and Communication Technology |

| Acronym | Full Meaning |
|---|---|
| LRA | Labour Relations Act |
| CoGTA | Department of Cooperative Governance and Traditional Affairs |
| DPP | Director of Public Prosecutions |

### 5. Cross-Referencing Clause

5.1. All references in this Policy to *Annexures, Schedules, or Appendices* shall be construed as integral parts of the Policy.

5.2. Where an Annexure or Form prescribes a specific process, such form or annexure shall have binding effect and shall be implemented in full.

### 6. Purpose of Definition Part

6.1. The definitions contained herein form the interpretive backbone of this Policy. No section, clause, or provision shall be applied in isolation from these definitions.

6.2. In all disciplinary or legal proceedings arising under this Policy, these definitions shall serve as the authoritative reference point for determining intent, scope, and liability.

## PART III

## POLICY RATIONALE AND JUSTIFICATION

### 1. Introduction

1.1. **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)** recognises that in the modern political environment, **information is both power and vulnerability**.

1.2. As a political organisation committed to ethical leadership, social justice, and African unity, AAAIC must safeguard its internal deliberations, strategic documents, and operational plans from exposure, manipulation, or unauthorised use.

1.3. The implementation of this **All-Inclusive Non-Disclosure Agreement (NDA) Policy** is therefore not a matter of administrative convenience, but a **constitutional, strategic, and moral necessity**.

1.4. This Policy stands as a bulwark against internal and external risks that threaten the integrity, credibility, and operational survival of the movement. It provides a binding covenant of trust among all who serve the organisation — from the National Executive Committee (NEC) to the most local branch committee.

## 2. The Philosophical and Ethical Foundation

2.1. The principle of **confidentiality** is anchored in both **African communal ethics** and universal governance traditions. In African political culture, wisdom and counsel are shared in confidence within the council (*lekgotla*) until collective decisions are finalised for public communication.

2.2. Confidentiality therefore does not contradict transparency — rather, it is the **ethical discipline that protects the integrity of the decision-making process** before outcomes are made public.

2.3. AAAIC, as a movement founded on honesty, discipline, and integrity, affirms that **trust is the currency of leadership**. The preservation of confidentiality is thus an expression of loyalty, respect, and collective responsibility.

2.4. Without a structured confidentiality regime, organisations fall prey to **factionalism, misinformation, infiltration, and reputational erosion** — all of which undermine democratic functioning.

2.5. Philosophically, this Policy embodies the **Ubuntu principle** — *"I am because we are"* — affirming that loyalty to the collective interest supersedes individual publicity or gain. It ensures that all members protect the dignity of the organisation as they would their own.

## 3. Strategic Justification

3.1. The AAAIC operates within a **competitive political landscape** where strategic intelligence, campaign methodologies, and organisational innovations constitute critical assets.

3.2. Leakage or unauthorized disclosure of internal strategies may:

(a) Compromise electoral and policy initiatives;
(b) Undermine negotiations with allies, coalitions, or stakeholders;
(c) Expose internal vulnerabilities to adversarial entities; and
(d) Erode public trust and credibility.

3.3 The adoption of this NDA Policy ensures a **systemic approach to information protection**, preventing ad-hoc or inconsistent practices across branches and tiers.

3.3. Strategically, it aligns the organisation's internal governance with the best practices of mature political institutions globally — recognising that **confidentiality and transparency are not opposites but sequential phases of integrity**.

3.4. This Policy therefore serves as an instrument for **operational resilience**, **institutional coherence**, and **long-term sustainability** of AAAIC's political agenda.

## 4. Risk Context and Organisational Vulnerability

4.1. Political organisations are inherently vulnerable to information-related risks, including:

- Deliberate leaks by insiders;
- Accidental exposure through negligence or poor digital security;
- Cyber-attacks targeting communications infrastructure;
- Breaches of donor confidentiality; and
- Misrepresentation of internal deliberations by external actors.

4.2. Each of these risks carries severe potential consequences — ranging from financial loss and electoral disadvantage to reputational collapse and legal exposure.

4.3. The AAAIC acknowledges that information mismanagement is equivalent to **institutional self-harm**. As such, this Policy establishes layered protective mechanisms covering classification, authorisation, and enforcement.

4.4. A comprehensive confidentiality framework also deters opportunism and reinforces the ethical responsibility of every member to protect collective integrity.

4.5. The **absence of a unified NDA policy** has historically led to inconsistencies and vulnerabilities within political formations in South Africa — including unauthorised publication of internal documents, premature media leaks, and manipulation of party communications for factional gain.

4.6. This Policy thus pre-emptively eliminates such weaknesses by embedding confidentiality obligations into the **DNA of the organisation**.

## 5. Jurisprudential and Legal Precedent

5.1. The principles enshrined in this Policy draw legitimacy from the jurisprudence of South African courts, which recognise **confidentiality as a cornerstone of fiduciary and contractual relationships**.

5.2. In **President of the Republic of South Africa and Others v South African Rugby Football Union (1999 (4) SA 147 (CC))**, the Constitutional Court affirmed that individuals entrusted with sensitive information owe a **duty of confidentiality** that arises from the nature of their office and the trust reposed in them.

5.3. Similarly, in **Myeni v South African Airways SOC Ltd (2020 (2) SA 523 (GJ))**, the High Court held that board members who disclose confidential board deliberations breach their fiduciary obligations and may face removal or liability.

5.4. These precedents underline that **disclosure of privileged information by officials constitutes misconduct**, and that organisations are entitled to impose contractual and disciplinary measures to protect their information.

5.5. Under **common law**, a duty of confidentiality arises whenever one party discloses information to another in circumstances that reasonably impose an obligation to maintain secrecy.

5.6. The courts have consistently upheld the **right of organisations to safeguard proprietary or strategic information**, even in the context of political and civil society entities.

5.7. The AAAIC's NDA Policy therefore stands on solid legal ground, harmonising organisational ethics with jurisprudential precedent and constitutional rights to privacy, dignity, and organisational autonomy.

## 6. Balancing Transparency and Confidentiality

6.1. A common misconception equates confidentiality with secrecy or suppression of information. However, this Policy recognises that **transparency and confidentiality are complementary principles** within good governance.

6.2. **Transparency** ensures accountability to the public and members regarding outcomes and decisions, while **confidentiality** ensures that deliberative processes occur in a secure, disciplined environment free from external interference or misrepresentation.

6.3. In this balance, AAAIC maintains that:

- Members are entitled to know final resolutions, but not necessarily internal deliberations or tactical details;
- The media and public have a right to accurate information, not premature leaks;
- Donors and partners deserve privacy within the confines of statutory disclosure requirements; and
- Confidentiality protects members' dignity during disciplinary or investigative processes.

6.4. This Policy therefore seeks to **institutionalise maturity in political communication** — promoting transparency in outcomes while securing confidentiality in processes.

6.5. Such equilibrium ensures **public confidence, legal compliance, and organisational cohesion**.

## 7. Organisational Integrity and Discipline

7.1. AAAIC regards confidentiality as a manifestation of discipline, not as an instrument of control.

7.2. Discipline is the cornerstone of effective political mobilisation; it requires that members act in unison, guided by collective decisions rather than personal agendas.

7.3. Information leaks often originate from **individual ambition, factional interest, or external influence**, which erode collective strength.

7.4. Through this Policy, AAAIC codifies confidentiality as part of its **Code of Conduct**, making disclosure breaches a disciplinary offence akin to insubordination or misconduct.

7.5. This institutional discipline strengthens organisational cohesion and reinforces respect for collective decisions, ensuring that leadership structures can operate without fear of betrayal or manipulation.

## 8. Confidentiality as a Governance Imperative

8.1. In political governance, confidentiality is not merely administrative — it is **a governance principle necessary for lawful, effective, and ethical management of information**.

8.2. It enables leaders to deliberate candidly, make decisions based on evidence, and protect sensitive stakeholder relationships.

8.3. Without confidentiality:

- Governance structures become paralysed by fear of exposure;
- Members lose confidence in the integrity of processes; and
- Opponents exploit internal weaknesses to discredit leadership.

8.4. The NDA Policy thus operationalises the **governance principle of informed trust** — empowering leaders to act responsibly while maintaining accountability.

8.5. It reinforces the concept that governance is a **shared trust**, where each member is a custodian of the organisation's reputation and internal security.

## 9. Information Security and the Digital Context

9.1. The contemporary political environment operates within a **digital ecosystem**, where data transmission occurs across multiple platforms — often outside formal organisational control.

9.2. The proliferation of social media, instant messaging, and digital file-sharing poses unprecedented risks to organisational confidentiality.

9.3. A single screenshot, forwarded message, or cloud-stored document can expose an entire strategy.

9.4. The AAAIC therefore recognises the imperative to **embed cybersecurity and digital discipline within its confidentiality framework**.

9.5. This Policy integrates with the organisation's ICT and Data Protection policies to:

- Enforce access controls;
- Mandate encryption and password security;
- Prohibit sharing of confidential materials through unauthorised digital channels; and
- Hold individuals accountable for digital negligence leading to data exposure.

9.6. In this regard, confidentiality transcends moral duty — it becomes a **technical and operational obligation**, enforceable by internal and statutory mechanisms.

## 10. Protection of Organisational Reputation

10.1. Reputation is the lifeblood of any political movement. The AAAIC's credibility rests on public trust in its leadership integrity, internal stability, and ethical conduct.

10.2. Reputational harm resulting from unauthorised disclosures can have long-term consequences, including loss of donor confidence, electoral disadvantage, and diminished public influence.

10.3. This Policy establishes a framework for **reputation protection** by ensuring that sensitive matters are handled responsibly and communicated through authorised channels.

10.4. It also fosters a culture of professionalism and discretion, especially among spokespersons, media liaisons, and representatives authorised to engage with the public.

10.5. The protection of organisational reputation is therefore not a peripheral concern but a **strategic security function** integral to AAAIC's survival and growth.

## 11. Alignment with National and International Standards

11.1. This Policy aligns AAAIC's governance with **South Africa's constitutional and legislative framework**, particularly those governing privacy, data protection, and organisational accountability.

11.2. Internationally, it is consistent with principles drawn from:

- The **African Union Convention on Cyber Security and Personal Data Protection (2014)**;
- The **United Nations Convention Against Corruption (2003)**; and

- Global best practices for political party governance endorsed by the **Inter-Parliamentary Union (IPU)** and **Transparency International**.

11.3. By adopting this Policy, AAAIC positions itself as a **model of ethical governance**, showcasing African political maturity grounded in confidentiality, respect, and integrity.

## 12. Concluding Justification

12.1. The justification for this Policy is both **pragmatic and principled**. It arises from the need to protect the AAAIC's internal processes while demonstrating to the public that the movement upholds professionalism and integrity.

12.2. The NDA Policy is therefore not a restriction but a **guarantee of trust** — enabling free, candid internal dialogue while ensuring collective responsibility in communication.

12.3. It embodies the AAAIC's belief that **ethical leadership begins with disciplined silence, followed by transparent truth**.

12.4. The existence of this Policy reinforces the message that the AAAIC is a **responsible custodian of information**, worthy of the confidence of its members, supporters, and the nation at large.

12.5. Through this instrument, AAAIC declares that confidentiality is not secrecy, but **an honourable covenant of stewardship** — a sacred trust that binds every member to the collective destiny of the movement.

**PART IV**

**POLICY APPLICATION**

## 1. General Scope of Application

1.1. This Non-Disclosure Agreement (NDA) Policy applies **uniformly and comprehensively** across all organisational structures, tiers, and functional domains of **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)**.

1.2. The Policy is **binding** on every person who, by virtue of their position, access, or association with the organisation, obtains or is exposed to information designated as confidential, privileged, restricted, or internal.

1.3. Compliance with this Policy is **mandatory**, not discretionary. The duty of confidentiality arises automatically upon assumption of office, engagement in organisational activities, or receipt of confidential information, whether or not a formal NDA has yet been signed.

1.4. The provisions herein shall **supersede any inconsistent confidentiality undertakings** previously executed, save where such undertakings impose stricter obligations consistent with this Policy.

1.5. The Policy applies irrespective of whether information is stored, transmitted, or communicated **verbally, digitally, in writing, or by observation**.

## 2. Tiers of Application

2.1. For administrative clarity, this Policy shall apply at the following organisational tiers:

(a) **National Tier:**
The National Congress, National Executive Committee (NEC), National Working Committee (NWC), National Integrity Committee, and all national sub-structures and commissions.

(b) **Provincial Tier:**
The Provincial Executive Committees (PECs), Provincial Working Committees (PWCs), and all provincial sub-committees or appointed task teams.
(c) **Regional Tier:**
The Regional Executive Committees (RECs), Regional Working Committees (RWCs), and related administrative and disciplinary organs.

(d) **Local and Branch Tier:**
Branch Executive Committees (BECs), Branch General Meetings, and sub-structures established at ward or community level.

(e) **Associated Formations:**
Youth Wing, Women's Wing, Veterans League, Student Movement, and all thematic or sectoral arms under the authority or recognition of AAAIC.

(f) **Special and Ad Hoc Committees:**
All committees appointed for specific investigations, policy drafting, disciplinary hearings, or organisational reviews.

2.2. Every tier shall incorporate the principles of this Policy into its **Terms of Reference, Standing Rules, and Codes of Conduct**, ensuring harmonised enforcement.

## 3. Categories of Covered Individuals

3.1. The duty of confidentiality and the enforcement provisions of this Policy extend to the following categories of persons:

(a) **Elected and Appointed Officials:**
All members holding positions within the NEC, PEC, REC, BEC, or any committee created by the organisation.

(b) **Employees and Staff:**
All permanent, part-time, or contract employees of AAAIC at any level, including administrative, financial, and technical personnel.

(c) **Volunteers and Interns:**
Any person offering unpaid service, internship, or temporary assistance who, in that capacity, may access or be exposed to confidential information.

(d) **Consultants and Service Providers:**
External experts, auditors, legal advisors, or contractors engaged to perform services for or on behalf of AAAIC.

(e) **Allied Partners and Collaborators:**
Coalition partners, NGOs, think-tanks, or institutions with which AAAIC shares joint initiatives or information under formal or informal cooperation.

(f) **Former Members and Officials:**
Individuals who have previously served within any capacity of the organisation, insofar as confidential information obtained during their tenure remains undisclosed.

(g) **Third-Party Associates:**
Any person indirectly exposed to AAAIC information through proximity, technical access, or delegated representation (e.g., interpreters, security staff, drivers, or IT technicians).

3.2. The confidentiality obligations imposed under this Policy **continue beyond the termination** of employment, membership, or service. Information obtained during engagement remains protected indefinitely unless lawfully released by the NEC.

## 4. Functional Domains of Application

4.1. This Policy applies across all operational and functional domains of the organisation, including but not limited to:

(a) **Strategic Planning and Political Affairs:**
Policy formulation, electoral strategy, coalition negotiations, and internal communications between decision-making bodies.

(b) **Finance and Fundraising:**
Budget deliberations, donor information, fundraising strategies, and any document revealing sources or uses of funds not intended for public disclosure.

(c) **Membership Administration:**
Databases, registers, and internal reports containing personal data, contact details, or disciplinary records of members.

(d) **Communications and Media Relations:**
Internal press drafts, media strategies, talking points, or social-media plans not yet authorised for public release.

(e) **Legal and Disciplinary Processes:**
Complaints, investigations, arbitration, and legal advice obtained in confidence.

(f) **Human Resources and Organisational Development:**
Recruitment processes, performance evaluations, and internal restructuring plans.

(g) **Information Technology and Digital Systems:**
Passwords, network architecture, databases, and internal correspondence systems.

(h) **Security and Intelligence:**
Information related to security operations, surveillance, threat assessments, and protective arrangements for leadership and events.

4.2. All directors of these functional domains bear a **fiduciary obligation** to ensure that confidentiality procedures are operationalised through written NDAs and regular training.

## 5. Policy Applicability to Information Types

5.1. This Policy governs all forms of **Confidential Information**, regardless of medium, including:

(a) Documents labelled *Confidential*, *Internal*, *Restricted*, or *For Official Use Only*;
(b) Minutes of internal meetings not cleared for public release;
(c) Electronic communications, databases, or records containing sensitive data;
(d) Recordings, transcripts, and working notes;
(e) Strategic plans, draft policies, research reports, and election materials;
(f) Personal or biometric data of members, donors, and stakeholders;
(g) Passwords, encryption keys, or authentication tokens; and
(h) Oral or observed communications during restricted sessions.

5.2. The **form of communication** does not determine confidentiality. Information conveyed verbally in a closed meeting or seen incidentally on a screen is equally protected as a formal document.

5.3. When doubt exists about whether information is confidential, it shall be **presumed confidential** until clarified in writing by the relevant authority.

## 6. Territorial Application

6.1. This Policy applies to all activities and persons operating **within or outside the Republic of South Africa** on behalf of AAAIC.

6.2. Members representing the organisation abroad in meetings, diplomatic exchanges, or international collaborations shall remain bound by the same confidentiality obligations.

6.3. Any information shared internationally must comply with **South African privacy legislation** and the AAAIC's internal data-transfer protocols.

## 7. Application to Organisational Committees

7.1. Each committee, whether standing or ad hoc, must adopt **specific confidentiality undertakings** for its members before commencement of its work.

7.2. Such undertakings shall affirm:

(a) Understanding of the NDA Policy;
(b) Commitment to non-disclosure; and
(c) Acknowledgment of disciplinary and legal consequences in case of breach.

7.3. Committee chairs are accountable for ensuring that members observe confidentiality, and they must brief members at the start and end of each meeting on confidentiality requirements.

7.4. Minutes of confidential sessions shall be **classified and stored separately** from general records, accessible only to authorised officers.

7.5. Where external experts or witnesses are invited to appear before any committee, they must sign a **Confidentiality Undertaking Form (Annexure C)** prior to participation.

**8. Application to Contractors and Service Providers**

8.1. All contractors, suppliers, or consultants engaged by AAAIC shall be required to execute a **Non-Disclosure Agreement** consistent with this Policy prior to commencement of work.

8.2. Such NDA shall bind:

- The contractor's employees, subcontractors, and affiliates;
- Any third parties to whom work may be delegated; and
- The contractor's successors and assigns.

8.3. Contractors must ensure that **confidential information received from AAAIC is used solely for contract performance**, and returned or destroyed upon completion.

8.4. Breach of confidentiality by a contractor constitutes **material breach of contract**, entitling AAAIC to terminate the agreement, seek damages, and blacklist the contractor from future engagements.

8.5. The Procurement and Legal Departments shall maintain **records of all executed NDAs**, subject to periodic compliance audits.

## 9. Application to Coalition Partners and External Entities

9.1. Where AAAIC enters into partnerships, coalitions, or joint initiatives with other political parties, civil society organisations, or research entities, the exchange of information shall be governed by **a Memorandum of Understanding (MoU)** incorporating confidentiality clauses consistent with this Policy.

9.2. Partners shall be informed in writing of the **classification level** of any information shared, and their obligation to protect it from disclosure or misuse.

9.3. No AAAIC member shall transmit internal communications, minutes, or strategic data to an external partner without prior **written authorisation** from the NEC or delegated authority.

9.4. Breaches by partners or affiliates may lead to suspension or termination of cooperation, and where applicable, **civil or criminal proceedings**.

## 10. Application to Former Members and Officials

10.1. The confidentiality obligation extends **beyond the term of office or membership**.

10.2. Former members, officials, and employees shall not:

(a) Disclose confidential information acquired during their tenure;
(b) Use such information for personal gain or to the detriment of AAAIC; or
(c) Publish or communicate internal materials without NEC consent.

10.3. The organisation reserves the right to **seek injunctive relief or damages** against any former official or member who breaches confidentiality after disengagement.

10.4. The handover process upon resignation, suspension, or removal shall include a **Confidentiality Exit Declaration**, confirming that all organisational records have been surrendered and no copies retained.

## 11. Application in Disciplinary and Investigative Processes

11.1. All disciplinary proceedings, internal investigations, and mediation sessions are confidential by nature.

11.2. Parties involved shall refrain from discussing or publicising such matters outside authorised channels.

11.3. The confidentiality duty applies equally to:

- Complainants and respondents;
- Witnesses and representatives; and
- Investigating or adjudicating officers.

11.4. Violation of confidentiality in such processes constitutes **separate misconduct**, irrespective of the outcome of the underlying case.

## 12. Temporal Application

12.1. This Policy applies from the date of its formal adoption by the **National Executive Committee** and remains in force until amended or replaced.

12.2. All existing NDAs within the organisation shall be deemed **incorporated by reference** into this Policy and shall continue to operate under its authority.

12.3. The confidentiality obligations described herein are **perpetual**, surviving termination of engagement, closure of committees, or dissolution of sub-structures.

## 13. Enforcement Responsibility

13.1. Each organisational tier shall designate a **Confidentiality Compliance Officer** responsible for:

(a) Administering NDAs;
(b) Conducting induction briefings;
(c) Reporting breaches; and
(d) Coordinating with the Integrity and Legal Affairs Units.

13.2. The National Integrity Committee shall serve as the **central oversight body**, ensuring consistent enforcement and maintaining a registry of executed NDAs and reported breaches.

13.3. All officers shall ensure that **no individual is given access to confidential information** without first acknowledging this Policy and signing the requisite undertaking.

## 14. Exceptions and Authorised Disclosure

14.1. Disclosure of confidential information may occur only when:

(a) **Expressly authorised** in writing by the NEC;
(b) **Legally compelled** by court order or statutory obligation;
(c) **Necessary for internal reporting**, provided it remains within authorised channels; or
(d) **Required to prevent imminent harm** to life, security, or property, subject to post-disclosure reporting.

14.2. Even in authorised disclosures, only the **minimum necessary information** shall be released.

14.3. Any uncertainty regarding permissible disclosure shall be referred to the **Legal Affairs Directorate** for written clarification.

### 15. Binding Effect

15.1. Every person to whom this Policy applies shall be deemed to have accepted its terms upon participation in any organisational activity, irrespective of formal signature.

15.2. Ignorance of the Policy or failure to read it shall **not exempt** any individual from accountability.

15.3. All organisational handbooks, codes, and induction materials shall incorporate this Policy by reference to ensure **continuous awareness and enforceability**.

## PART V

## OBLIGATIONS OF MEMBERS AND OFFICIALS

### 1. General Duty of Confidentiality

1.1. Every member, office bearer, employee, and associate of **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)** shall owe a continuing **duty of confidentiality** to the organisation in respect of all information, communications, documents, and deliberations that are not authorised for public disclosure.

1.2. This duty arises automatically from the individual's relationship of trust with the organisation, regardless of whether a written agreement has been signed.

1.3. The duty extends to all forms of information, whether written, electronic, oral, visual, or otherwise, and whether obtained deliberately or incidentally.

1.4. The obligation to maintain confidentiality shall survive:

(a) Suspension or expulsion from membership;
(b) Termination of employment or service;
(c) Dissolution of any committee or structure; and
(d) The cessation of office or engagement in any capacity within the organisation.

## 2. Ethical Standards and Conduct Expectations

2.1. Every person bound by this Policy shall conduct themselves with **integrity, discretion, and loyalty** in all dealings relating to organisational information.

2.2. The following conduct principles shall guide all members and officials:

(a) **Integrity:** Confidential information shall be used solely for authorised organisational purposes and never for personal, political, or financial advantage.

(b) **Loyalty:** Members shall prioritise the interests of the organisation over individual or factional agendas when handling sensitive information.

(c) **Discretion:** No person shall discuss, reproduce, or reference confidential information in public, private, or informal settings, including on digital or social media platforms.

(d) **Responsibility:** Every member must take active measures to protect organisational information under their control.

(e) **Accountability:** Members and officials are personally liable for any breach, negligence, or omission that results in the disclosure or loss of confidential data.

2.3. Conduct inconsistent with these ethical standards constitutes **misconduct** and may attract disciplinary or legal sanctions in accordance with Part XI of this Policy.

## 3. Specific Obligations of Members

3.1. Members of the AAAIC, whether holding office or not, are required to:

(a) Respect and uphold the confidentiality of all internal discussions, resolutions, and communications;
(b) Avoid sharing internal deliberations or disputes on social or public media platforms;
(c) Refrain from forwarding internal emails, minutes, or strategy documents to unauthorised persons;

(d) Protect the organisation's reputation by ensuring no confidential information is used to discredit the movement;
(e) Comply fully with any directives from authorised officers regarding the handling or classification of documents; and
(f) Report any suspected breach of confidentiality through approved channels.

3.2. Members who become aware of any unauthorised disclosure, or who suspect an impending breach, shall have an **affirmative duty to report** such matter to the relevant Confidentiality Compliance Officer or Integrity Committee.

3.3. The **failure to report** a known or suspected breach constitutes an act of negligence and may itself be treated as a disciplinary offence.

## 4. Obligations of Office Bearers and Officials

4.1. Office bearers, including those serving in the National Executive Committee (NEC), Provincial Executive Committees (PECs), Regional and Branch structures, owe a **heightened fiduciary obligation** to protect organisational information.

4.2. Such officials shall:

(a) Ensure that confidential materials are circulated only among authorised recipients;
(b) Classify sensitive information appropriately and mark documents "CONFIDENTIAL" where applicable;
(c) Secure meeting minutes, recordings, and reports under restricted access;
(d) Refrain from discussing confidential deliberations outside designated forums;
(e) Exercise restraint in public commentary relating to internal matters; and
(f) Ensure that subordinates, assistants, and advisors under their authority understand and comply with this Policy.

4.3. An official who authorises or tolerates the disclosure of confidential information by subordinates shall be deemed **vicariously liable** for such breach, except where it is shown that adequate preventive measures were taken.

4.4. Members of leadership structures must lead by example, cultivating a culture of confidentiality through **consistent discipline, discretion, and accountability**.

## 5. Obligations of Employees, Staff, and Contractors

5.1. Employees and contracted service providers shall:

(a) Sign a written Non-Disclosure Agreement prior to accessing any confidential material;
(b) Use confidential information strictly within the scope of their employment or contract
(c) Store documents securely, both physically and digitally, and ensure password protection;
(d) Return or delete all organisational materials upon termination of employment or completion of service; and
(e) Avoid retaining or duplicating documents for private purposes.

5.2. Any staff member who leaves employment or is reassigned shall complete a **Confidentiality Exit Declaration**, certifying that they retain no organisational information.

5.3. Contractors and consultants who engage sub-contractors shall bear full responsibility for ensuring that all subordinates observe identical confidentiality standards.

## 6. Obligations of Committee Members

6.1. Members serving on any AAAIC committee — including disciplinary, investigative, electoral, or ad hoc bodies — are bound by a **committee-level confidentiality duty** that extends beyond their normal membership obligations.

6.2. They shall:

(a) Treat all committee proceedings as privileged and non-public;
(b) Safeguard documentation, witness statements, and deliberative records;
(c) Ensure that minutes or recordings are submitted to the Secretariat through secure channels; and

(d) Avoid discussing ongoing committee matters with unauthorised persons, including members not serving on that committee.

6.3. Any leak of committee information, findings, or internal deliberations constitutes **gross misconduct** and may warrant suspension, expulsion, or legal action.

6.4. Committee chairs bear overall accountability for briefing members about confidentiality expectations before each session.

## 7. Obligations of Spokespersons and Public Representatives

7.1. Spokespersons, media liaisons, and other representatives authorised to communicate on behalf of AAAIC must adhere strictly to the boundaries of their mandate.

7.2. They shall:

(a) Publicly communicate only information that has been approved or cleared by the NEC or authorised communication directorate;
(b) Decline to comment on internal matters not designated for public disclosure;
(c) Avoid speculative or personal interpretations of confidential decisions; and
(d) Ensure accuracy and consistency in messaging to protect organisational credibility.

7.3. Spokespersons who inadvertently receive confidential information outside their official scope shall immediately report it to their supervising authority and refrain from further dissemination.

## 8. Duty to Secure and Manage Information

8.1. Every person covered by this Policy shall adopt **reasonable and practical measures** to secure confidential information, including:

(a) Storing documents in locked cabinets or password-protected systems;
(b) Avoiding use of personal devices or public Wi-Fi for confidential communications;
(c) Employing encryption or secure transmission methods for digital files;
(d) Restricting printing or copying of confidential materials to authorised needs; and
(e) Shredding or securely deleting obsolete documents.

8.2. Digital security responsibilities include:

(a) Using strong, unique passwords;
(b) Avoiding sharing login credentials;
(c) Ensuring two-factor authentication where available;
(d) Reporting phishing or data-breach incidents immediately; and
(e) Complying with the organisation's ICT and Data Protection Policies.

8.3. Failure to maintain reasonable safeguards that lead to data exposure constitutes **negligent breach of confidentiality** and attracts disciplinary action.

## 9. Duty to Report Breaches and Suspected Violations

9.1. Every member and official has a **mandatory duty** to report any actual or suspected breach of confidentiality within twenty-four (24) hours of discovery.

9.2. Reports shall be submitted in writing to the designated **Confidentiality Compliance Officer** or directly to the **Integrity and Legal Affairs Directorates**.

9.3. Reports must include:

(a) A detailed description of the suspected breach;
(b) Identities of persons involved;
(c) Nature of the information compromised;
(d) Date, time, and method of occurrence; and
(e) Any immediate corrective measures taken.

9.4. Whistleblowers reporting in good faith shall be protected from retaliation under AAAIC's **Whistleblower Protection Policy**.

9.5. However, malicious or false reporting intended to defame another member shall constitute misconduct.

## 10. Restrictions on Personal Use of Organisational Information

10.1. Confidential information obtained through membership or service within AAAIC shall **not be used for personal, political, or financial benefit**, including but not limited to:

(a) Influencing external organisations or media for self-promotion;
(b) Gaining advantage in electoral contests or appointments;
(c) Benefiting a faction, third party, or external competitor; or
(d) Engaging in business ventures or solicitations using privileged data.

10.2. Members are prohibited from publishing or sharing internal materials such as meeting minutes, campaign strategies, or internal circulars on any personal platform without written authorisation.

10.3. Any such unauthorised use constitutes **gross abuse of organisational trust** and may attract disciplinary and legal consequences.

## 11. Duty of Non-Disclosure in Public and Digital Spaces

11.1. Members shall refrain from discussing or referencing confidential matters on:

(a) Social media platforms (Facebook, X, WhatsApp, TikTok, etc.);
(b) Radio, television, or press interviews;
(c) Public forums, conferences, or community meetings; and
(d) Any online group not formally sanctioned by the organisation.

11.2. Posts, comments, or messages that reveal internal disputes, deliberations, or sensitive communications constitute **unauthorised disclosure** even if made indirectly or without naming the organisation.

11.3. Digital communications must conform to the same standard of confidentiality as written documents, and screenshots or recordings of internal discussions are strictly prohibited.

## 12. Joint and Vicarious Liability

12.1. Where a breach of confidentiality arises from joint participation, all involved persons shall bear **joint and several liability**.

12.2. Leadership figures who fail to enforce confidentiality standards among subordinates may be held **vicariously responsible** for resulting disclosures.

12.3. In assessing liability, AAAIC shall consider:

(a) The role and authority of the person involved;
(b) The degree of negligence or intent; and
(c) The harm caused to the organisation’s interests.

12.4. Liability under this Policy does not preclude **civil action for damages** or **criminal prosecution** where applicable.

## 13. Obligation to Cooperate in Investigations

13.1. All members, officials, and employees shall fully cooperate in any investigation concerning a suspected breach of confidentiality.

13.2. Cooperation includes providing truthful statements, surrendering relevant documents, and attending hearings or inquiries when summoned.

13.3. Obstructing or refusing to cooperate with such investigations constitutes **insubordination and misconduct**.

13.4. Confidentiality shall continue to apply during the investigation process — information about ongoing cases shall not be disclosed externally without authorisation.

## 14. Obligation to Undergo Training and Awareness

14.1. Every person bound by this Policy shall participate in **mandatory induction and refresher training** on confidentiality and data protection.

14.2. The training shall cover:

(a) Understanding the scope of confidential information;
(b) Risks associated with disclosure;
(c) Reporting mechanisms; and
(d) Disciplinary consequences for violations.
14.3 Completion of such training shall be a **prerequisite for office assumption** and periodic reappointment to sensitive positions.

14.3. The Human Resources Directorate shall maintain training records and monitor compliance across all tiers.

## 15. Obligation to Preserve Organisational Property

15.1. All confidential records, whether in hard or soft copy, are the **exclusive property of AAAIC**.

15.2. Members and officials are custodians, not owners, of the information entrusted to them.

15.3. Upon termination of engagement, individuals shall:

(a) Return all physical and digital records in their possession;
(b) Permanently delete organisational data from personal devices; and
(c) Certify compliance in writing to the responsible officer.
15.4 Retention or duplication of records after disengagement is strictly prohibited and may lead to civil or criminal remedies.

## 16. Sanctions for Non-Compliance

16.1. Breach of any obligation under this Policy constitutes a **disciplinary offence**, punishable by measures including:

(a) Verbal or written warning;
(b) Suspension from duties;
(c) Removal from office;
(d) Expulsion from membership; and
(e) Civil or criminal proceedings for damages.

16.2. The gravity of the sanction shall correspond to the nature, extent, and consequence of the breach.

16.3. Repeated or wilful breaches may result in permanent disqualification from holding any position of trust within AAAIC.

## 17. Moral Obligation and Oath of Confidentiality

17.1. In addition to legal and contractual duties, every member and official owes a **moral duty of silence and fidelity** to the movement.

17.2. Upon joining or assuming office, each person shall take an **Oath of Confidentiality**, pledging loyalty to the organisation’s values and commitment to protect its internal affairs.

17.3. The Oath shall read substantially as follows:

"*I, [Name], solemnly pledge to maintain the confidentiality of all matters entrusted to me by the ARISE AFRIKA ARISE INDEPENDENT CONGRESS.*

*I shall not, without lawful authority, disclose or misuse any information obtained in my capacity as a member or official.*

*I affirm my loyalty to the organisation, its mission, and its ethical values, and undertake to protect its dignity and integrity at all times*."

17.4. The taking of this Oath symbolises **honourable stewardship**, reinforcing that confidentiality is not secrecy, but disciplined protection of the collective trust.

## PART VI

## INFORMATION CLASSIFICATION, ACCESS, AND HANDLING PROCEDURES

### 1. Introduction

1.1. **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)** recognises that **information is a critical organisational asset**, and improper handling can cause irreparable harm to strategic, operational, legal, and reputational interests.

1.2. This Part establishes a **comprehensive framework for classifying, accessing, and handling organisational information** across all tiers and substructures of AAAIC.

1.3. These procedures ensure that **only authorised individuals gain access** to sensitive information and that its dissemination, storage, or destruction is conducted in a **controlled, auditable, and secure manner**.

1.4. This framework is applicable to all forms of information, including **oral communications, written documents, electronic files, recordings, and observed**

**content**, and complements the overarching obligations set out in Parts IV and V of this Policy.

## 2. Objectives of Information Classification

2.1. The objectives of information classification are to:

(a) Identify and categorise all information according to sensitivity and potential risk if disclosed;
(b) Protect confidential and strategic organisational material from unauthorised access;
(c) Establish clear **authorisation hierarchies** for viewing, handling, and dissemination
(d) Provide guidelines for secure handling, storage, transmission, and destruction;
(e) Ensure compliance with South African legislation, including the **Protection of Personal Information Act (POPIA, 2013)**, and other applicable regulatory frameworks; and
(f) Facilitate rapid identification and response in the event of information compromise.

## 3. Classification Categories

AAAIC establishes **four primary categories of information**, each with defined handling protocols:

### 3.1. Public Information

3.1.1. Definition: Information intended for dissemination to the public without restriction, including:

- Official press releases authorised by the NEC;
- Public policy statements;
- Event announcements and non-sensitive organisational reports.

3.1.2. Handling Requirements:

- Can be freely shared with external parties;
- No authorisation required for dissemination;
- Must maintain accuracy and consistency with authorised messages.

### 3.2. Confidential Information

3.2.1. Definition: Information intended for **internal use only**, access restricted to members or officials with a legitimate organisational need. Examples include:

- Internal meeting minutes not yet approved for public release;
- Draft policies, reports, or research;
- Membership data, internal correspondence, and preliminary strategic plans.

3.2.2. Handling Requirements:

- Access limited to authorised personnel as designated by the NEC or relevant committee;
- Must be marked *CONFIDENTIAL*;
- Cannot be disclosed outside authorised channels without written approval;
- Must be stored securely, either in locked cabinets (physical) or encrypted systems (digital).

### 3.3. Restricted Information

3.3.1. Definition: Information of higher sensitivity, whose disclosure could significantly compromise AAAIC's strategic, operational, or legal position. Examples include:

- Electoral or coalition strategies;
- Donor and financial agreements;
- Legal opinions or litigation strategy;
- Sensitive operational plans or personnel investigations.

3.3.2. Handling Requirements:

- Access limited to a defined group of senior officials or committee members;
- Must be marked *RESTRICTED*;
- Transmission must use secure channels (encrypted email, password-protected portals, or approved secure cloud systems);
- Printing or duplication requires explicit authorisation;

- Any storage outside authorised systems requires written approval.

### 3.4. Secret Information

3.4.1. Definition: Information of **critical organisational importance**, whose unauthorised disclosure could severely damage AAAIC, its members, or strategic operations. Examples include:

- High-level NEC deliberations prior to formal approval;
- Security protocols, risk assessments, and intelligence reports;
- Negotiation positions, sensitive coalition plans, and investigative findings.

3.4.2. Handling Requirements:

- Access restricted to NEC members, Integrity Committee, or authorised senior leadership;
- Must be marked *SECRET*;
- Strictly controlled distribution — physical copies limited and digitally encrypted;
- Transmission requires dual authorisation and use of secure portals;
- Destruction or archival requires documented approval;
- Breach is considered **gross misconduct** under Part XI of this Policy.

## 4. Authorisation Hierarchies

4.1. AAAIC establishes a **tiered authorisation framework** to control access to classified information:

| Classification | Access Level | Authorising Authority | Notes |
|---|---|---|---|
| Public | All members & general public | NEC or authorised spokesperson | No restrictions; maintain message consistency |
| Confidential | Functional committees, officers, specific members | Committee Chair / Department Head | Access limited to ‘need-to-know’ basis |
| Restricted | NEC, PEC Chairs, NWC | NEC or relevant | Access logged and recorded; dual |

| Classification | Access Level | Authorising Authority | Notes |
|---|---|---|---|
| | members | Director | authorisation recommended |
| Secret | NEC, Integrity Committee, authorised advisors | NEC (Chairperson) | Strictly controlled; all access logged; no unauthorised duplication |

4.2. All access, including digital retrieval or physical consultation, must be **documented in access logs** maintained by the Secretariat or Compliance Officers.

4.3. Requests for access beyond the standard hierarchy must be:

(a) Submitted in writing;
(b) Approved by the relevant authority; and
(c) Recorded for audit purposes.

**5. Digital Information Handling Protocols**

5.1. All digital confidential, restricted, or secret information must:

(a) Be stored in AAAIC-approved secure systems;
(b) Use strong passwords, multi-factor authentication, and encryption;
(c) Avoid personal or unsecured devices;
(d) Be shared only via secure channels approved by the ICT Directorate;
(e) Be backed up in a secure, access-controlled environment;
(f) Be immediately reported if accidental exposure occurs.

5.2. Email communications containing classified information must include **sensitivity markings** and a standard footer reminding recipients of the confidentiality obligation.

5.3. Cloud storage must comply with **POPIA standards**, ensuring personal data and strategic information remain protected from external access.

## 6. Physical Information Handling Protocols

6.1. Physical copies of confidential, restricted, or secret materials shall:

(a) Be stored in locked cabinets accessible only to authorised personnel;
(b) Be transported in secure containers;
(c) Be signed out using a logbook indicating the recipient, purpose, and return date;
(d) Not be left unattended in public areas or vehicles;
(e) Be destroyed securely when obsolete, using shredding or approved destruction methods.

6.2. Meeting rooms used for confidential or secret deliberations must:

- Restrict entry to authorised personnel;
- Prevent recording without permission;
- Ensure that all notes, documents, or electronic devices are removed after the meeting.

## 7. Handling of Orally Communicated Information

7.1. Oral communications of classified information are treated with the **same level of protection** as written or digital records.

7.2. Rules include:

(a) Avoid discussing confidential matters in public spaces or with unauthorised individuals;
(b) Use private rooms or secure digital platforms for teleconferences;
(c) Minimise the number of participants to essential personnel only;
(d) Recordings must be authorised, encrypted, and stored securely.

## 8. Handling of Third-Party Shared Information

8.1. Any confidential information received from external parties (donors, coalition partners, or consultants) is to be treated as **at least confidential within AAAIC**, unless otherwise classified.

8.2. Members must:

(a) Respect the original classification;
(b) Limit internal distribution to authorised personnel;
(c) Refrain from unauthorised disclosure;
(d) Report any suspected leakage or compromise.

8.3. Third-party NDAs shall be cross-referenced with this Policy to ensure **mutual confidentiality obligations** are observed.

## 9. Access Review and Auditing

9.1. Confidentiality Compliance Officers shall **periodically review access logs** to ensure adherence to classification protocols.

9.2. Reviews include:

(a) Verification of authorisation for all access events;
(b) Detection of anomalies or unauthorised attempts;
(c) Evaluation of security practices; and
(d) Recommendations for remedial action.

9.3. Non-compliance detected during audits will trigger **Part XI disciplinary procedures**, including corrective training or sanctions.

## 10. Handling During Organisational Transition

10.1. During leadership, committee, or staff transitions, the following protocols apply:

(a) All confidential, restricted, and secret information must be inventoried;
(b) Access credentials, keys, and passwords must be transferred or revoked under supervision;
(c) An exit declaration confirming no retention of information shall be completed by departing

members or staff;

(d) Digital systems access is revoked immediately upon disengagement.

10.2. Transitional breaches are considered **serious violations**, with immediate corrective action and investigation.

**11. Exceptions and Authorised Disclosures**

11.1 Disclosure outside the standard hierarchy is permitted only:

(a) With explicit written approval by the NEC;

(b) As required by law, including subpoenas or court orders;

(c) To protect life, safety, or property, with immediate reporting to the NEC;

(d) Within authorised internal committees on a **need-to-know basis**.

11.2 Even in authorised cases, only **the minimum necessary information** may be released, and such disclosures must be documented.

**12. Responsibilities of Classification Officers**

12.1 Classification Officers are responsible for:

(a) Assigning classification levels to new documents;

(b) Maintaining access control lists;

(c) Ensuring that digital and physical handling procedures are followed;

(d) Coordinating destruction of obsolete materials; and

(e) Reporting breaches or anomalies to the NEC and Integrity Committee.

12.2 Officers must receive **specialised training** and are accountable for lapses in classification and access control.

**13. Integration with NDA Policy Obligations**

13.1 Information classification, access, and handling procedures are **inseparable from the obligations under Parts IV and V** of this Policy.

13.2 Members, officials, and staff must adhere simultaneously to:

- Duty of confidentiality;
- Ethical standards;
- Reporting obligations; and
- Handling and storage protocols.

13.3 Failure to comply with classification rules constitutes a **disciplinary offence** and may trigger civil or criminal liability, depending on harm caused.

**14. Review and Amendment of Classification Protocols**

14.1 The NEC shall **review classification levels and handling procedures annually** or as necessary.

14.2 Adjustments may include:

(a) Updating categories to match operational or technological changes;

(b) Revising access hierarchies;

(c) Incorporating new security or legislative requirements; and

(d) Issuing circulars to inform all members and officials of changes.

14.3 All amendments shall be communicated formally and integrated into induction and refresher training.

## PART VIII — WHISTLEBLOWER PROTECTIONS AND REPORTING MECHANISMS

### 1. Introduction

1.1. **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)** recognises that **the integrity of its Non-Disclosure Agreement (NDA) Policy depends upon safe, transparent, and effective reporting mechanisms**.

1.2. Part VIII establishes a **comprehensive whistleblower protection framework** and outlines reporting procedures, rights, and safeguards for individuals who identify breaches, misconduct, or potential violations of confidentiality obligations.

1.3. This Part applies to all:

- Members, office bearers, and elected officials;
- Employees, contractors, and consultants;
- Committee and subcommittee participants; and
- External partners and stakeholders acting within AAAIC-related engagements.

1.4. These mechanisms ensure **organisational accountability, protection from retaliation, and compliance with ethical and legal obligations**, including the **Protected Disclosures Act, 2000 (Act No. 26 of 2000)** and relevant POPIA provisions.

## 2. Definition of Whistleblowing

2.1. Whistleblowing is the **good-faith disclosure** by a member, official, or affiliate of:

(a) Actual or suspected breach of the NDA Policy;
(b) Misuse or unauthorised disclosure of confidential, restricted, or secret information;
(c) Any misconduct or illegal activity compromising AAAIC's integrity; or
(d) Systemic failures that may jeopardise organisational operations or legal compliance.

2.2. Whistleblowing excludes:

- Malicious reporting intended to harm, defame, or manipulate outcomes;
- Reporting of trivial matters unrelated to confidentiality or integrity;
- Allegations without factual basis or supporting evidence.

## 3. Scope of Protection

3.1. Individuals who report in good faith are entitled to **protection from all forms of retaliation**, including:

(a) Dismissal, suspension, or demotion;
(b) Harassment, intimidation, or ostracism;
(c) Unfavourable alterations in duties, privileges, or access;
(d) Legal or administrative action instigated in reprisal;
(e) Threats to personal or family safety within organisational contexts.

3.2. Protection applies **regardless of whether the alleged breach is ultimately substantiated**, provided the disclosure is made honestly, without malicious intent.

3.3. Retaliatory conduct against whistleblowers constitutes a **separate breach of the NDA Policy** and may attract disciplinary action up to and including expulsion from the organisation.

## 4. Reporting Channels

4.1. AAAIC provides **multiple secure reporting channels** to accommodate confidentiality, accessibility, and urgency:

| Channel | Description | Security & Confidentiality Measures |
|---|---|---|
| Confidentiality Compliance Officer | Primary internal reporting officer for all NDA breaches | Secure email, encrypted submission portal, in-person confidential meeting |
| Integrity Committee | Secondary reporting channel, especially for senior-level issues | Secure record-keeping, restricted access to investigators only |
| Legal Affairs Directorate | Used for reporting breaches with potential legal consequences | Legal privilege protection, secure documentation and chain of custody |
| Anonymous Reporting Portal | Online encrypted platform for anonymous submissions | Ensures whistleblower identity is never disclosed, unless voluntarily revealed |

4.2. Reports must include, where possible:

(a) Description of the breach;
(b) Date, time, and location of occurrence;
(c) Identity of parties involved;
(d) Evidence supporting the allegation;
(e) Immediate corrective actions taken (if any); and
(f) Identity of the reporting individual (unless submitted anonymously).

## 5. Confidentiality of Reports

5.1. All whistleblower reports are treated as **highly confidential**.

5.2. Only authorised personnel directly involved in handling the report shall have access.

5.3. Disclosure of the whistleblower's identity to any person not authorised under this Policy constitutes **a serious violation** and triggers disciplinary measures.

5.4. Anonymous reports shall be investigated **to the fullest extent possible** without compromising the anonymity of the reporter.

## 6. Investigation of Whistleblower Reports

6.1. Upon receipt, reports shall be:

(a) Logged and assigned a unique tracking number;
(b) Reviewed by the Confidentiality Compliance Officer for preliminary assessment;
(c) Forwarded to the Integrity Committee for formal investigation, where appropriate.

6.3. Investigations must:

- Be conducted promptly and thoroughly;
- Maintain confidentiality of all parties involved;
- Document evidence, interviews, and findings;
- Protect the rights of both the whistleblower and the accused;
- Include risk mitigation measures to prevent recurrence.

6.4. The whistleblower shall be **kept informed** of the progress of the investigation, to the extent that it does not compromise confidentiality or the integrity of the process.

## 7. Interim Protections

7.1. While the investigation is ongoing, the whistleblower may request:

(a) Temporary reassignment;
(b) Restricted access to potential sources of conflict;
(c) Protective measures against harassment or intimidation; and
(d) Secure communication channels for correspondence and updates.

7.2. The Integrity Committee shall **assess and implement appropriate interim measures** to safeguard the whistleblower without prejudicing the investigation.

## 8. Prohibition of Retaliation

8.1. No person shall engage in retaliation, intimidation, or coercion against a whistleblower.

8.2. Retaliatory conduct includes, but is not limited to:

- Verbal threats or harassment;
- Social or professional ostracism;
- Unauthorised disclosure of the whistleblower's identity;
- Blocking access to duties, meetings, or decision-making processes;
- Initiating baseless disciplinary action against the whistleblower.

8.3. Retaliation triggers **immediate disciplinary action**, potentially including removal from office, suspension, or expulsion.

## 9. Verification and Good-Faith Standard

9.1. Whistleblower protection applies only to reports made in **good faith**, even if the allegations are unproven.

9.2. “Good faith” requires:

(a) Honest belief in the validity of the report;
(b) No personal motive for harm;
(c) Reasonable basis for suspicion or evidence; and
(d) Compliance with reporting procedures outlined in this Policy.
9.3 Malicious, frivolous, or reckless reporting constitutes a **separate disciplinary offence**.

## 10. Whistleblower Anonymity and Data Protection

10.1. AAAIC guarantees that personal information of whistleblowers shall:

(a) Be collected, stored, and processed securely;
(b) Be accessible only to authorised officers;
(c) Be protected from unauthorised digital or physical access;
(d) Be retained only as long as necessary for investigations and compliance purposes.

10.3. All electronic systems used for anonymous reporting must comply with **POPIA standards**, ensuring secure encryption, restricted access, and data integrity.

## 11. Integration with NDA Obligations

11.1. Whistleblower protections are **complementary to the NDA Policy**, not separate from it.

11.2. Reporting breaches of confidentiality does **not itself constitute disclosure** if conducted through authorised channels and in good faith.

11.3. Members reporting misconduct are **exempt from liability for disclosure** under this Policy, provided reporting is conducted in accordance with authorised procedures.

## 12. Accountability of Leadership

12.1. Leaders at all levels are responsible for:

(a) Encouraging reporting of breaches;
(b) Maintaining a non-retaliatory culture;
(c) Ensuring training and awareness on whistleblower rights;
(d) Monitoring implementation of protective measures; and
(e) Reporting systemic issues to the NEC for strategic response.

12.2. Leadership failure to protect whistleblowers may result in:

- Disciplinary action;
- Removal from office;
- Additional sanctions under AAAIC constitutional and legal provisions.

## 13. Training and Awareness

13.1. AAAIC shall provide mandatory **whistleblower training** as part of induction and annual refresher programs.

13.2. Training topics include:

(a) Identification of reportable breaches;
(b) Reporting channels and protocols;
(c) Protection measures and rights;
(d) Responsibilities of leaders in safeguarding whistleblowers;
(e) Ethical and legal obligations under South African law and AAAIC policy.

13.3. Completion of training is a prerequisite for holding office or accessing confidential information.

## 14. Record-Keeping and Reporting

14.1. The Integrity Committee and Legal Affairs Directorate shall maintain a **secure record of all whistleblower reports**, including:

(a) Submission details;
(b) Investigation notes;
(c) Interim measures;
(d) Outcomes and decisions;
(e) Documentation of any protective measures implemented.

14.2. Records shall be kept confidential, auditable, and retrievable for review, oversight, and compliance reporting.

## 15. Annual Reporting and Transparency

15.1. The NEC shall receive an **annual confidential report** on whistleblower activity, including:

(a) Number of reports received;
(b) Number and nature of investigations initiated;
(c) Outcomes, including sanctions applied;
(d) Lessons learned and systemic recommendations.

15.2. Reports shall be prepared without compromising whistleblower anonymity and without exposing sensitive organisational information.

**PART IX**

**REVIEW, AMENDMENT, AND POLICY IMPLEMENTATION**

## 2. Introduction

1.1. **ARISE AFRIKA ARISE INDEPENDENT CONGRESS (AAAIC)** recognises that **effective governance of confidential information requires continual oversight, periodic review, and structured implementation**.

1.2. Part IX establishes the **procedures and responsibilities** for reviewing, amending, and operationalising the NDA Policy across all organisational tiers, committees, and affiliates.

1.3. This Part ensures the Policy remains:

- Legally compliant;
- Operationally effective;
- Technologically current;
- Consistent with AAAIC strategic objectives; and
- Aligned with global best practices in information governance and confidentiality.

## 2. Policy Review Framework

2.1. The NEC shall ensure the NDA Policy undergoes **comprehensive review at least annually**, or sooner if:

(a) Legislative or regulatory changes occur;
(b) Significant breaches reveal procedural gaps;
(c) Organisational structural changes necessitate updates;
(d) New technologies or methods of information handling are adopted.

2.2. Review objectives include:

- Validating relevance and clarity of all definitions (Parts II & III);
- Ensuring obligations (Part V) remain enforceable;

- Verifying classification procedures (Part VI) remain effective;
- Confirming enforcement, sanctions, and whistleblower mechanisms (Parts VII & VIII) are functional;
- Identifying gaps, redundancies, or ambiguities in operational procedures;
- Ensuring cross-references with AAAIC constitution and legislative requirements are accurate.

2.3. Reviews shall be **formalised and documented**, including:

- Review date;
- Reviewing committee/officials;
- Proposed changes;
- Rationale for amendments;
- Approval signatures from NEC Chairperson and Secretary-General.

## 3. Amendment Procedures

3.1. Amendments to the NDA Policy may arise from:

(a) Recommendations from review exercises;
(b) NEC or subcommittee directives;
(c) Legal or regulatory updates;
(d) Lessons learned from breaches or enforcement proceedings.

3.2. Amendment proposals must be:

- Submitted in writing to the Policy Review Committee;
- Accompanied by a justification, impact assessment, and implementation plan;
- Reviewed in consultation with Legal Affairs Directorate, Compliance Officers, and NEC representatives.

3.3. Approval Process:

(a) Minor amendments (e.g., clarifications, typographical corrections) may be approved by the NEC directly;

(b) Major amendments (e.g., procedural or structural changes affecting multiple parts of the Policy) require:

- NEC deliberation;
- Vote according to AAAIC constitutional requirements;
- Ratification by the NEC Chairperson and Secretary-General;
- Notification to all members, committees, and relevant external partners.

3.4. All amendments are **documented, version-controlled, and integrated into the Policy manual**, with old versions archived for audit purposes.

## 4. Implementation Responsibilities

4.1. AAAIC assigns **clear responsibilities** to ensure effective operationalisation of the NDA Policy:

| Role | Responsibilities |
|---|---|
| NEC | Ultimate oversight; approval of amendments; enforcement endorsement; annual review coordination |
| Confidentiality Compliance Officer | Daily operational oversight; access control; reporting to NEC; training coordination |
| Integrity Committee | Investigation of breaches; adjudication recommendations; whistleblower protection oversight |
| Legal Affairs Directorate | Legal review of amendments; alignment with POPIA, Protected Disclosures Act, and other laws |
| Committee Chairs | Operational enforcement within committees; member training and awareness; reporting breaches |
| Secretariat | Policy documentation, distribution, record-keeping, and version control |

| Role | Responsibilities |
|---|---|
| Members & Officials | Adherence to obligations; participation in training; timely reporting of breaches |

4.2. The NEC shall conduct **annual evaluation** of responsibilities, identifying gaps in compliance, training, and reporting structures.

## 5. Policy Roll-Out and Awareness

5.1. AAAIC shall implement the NDA Policy across all tiers through a **structured roll-out plan**, including:

- Induction programs for new members;
- Annual refresher training for all office bearers and committees;
- Distribution of digital and printed copies;
- Notices of amendments, with mandatory acknowledgement of receipt.

5.2. Training shall cover:

(a) Definitions and scope of confidentiality;
(b) Obligations and conduct standards;
(c) Information classification and handling;
(d) Breach reporting, enforcement, and sanctions;
(e) Whistleblower rights and protections;
(f) Review and amendment procedures.

5.3 Training completion shall be **tracked and recorded**, and access to classified information may be conditioned upon certification of understanding and compliance.

## 6. Monitoring and Evaluation Metrics

6.1. AAAIC shall establish **quantitative and qualitative metrics** to assess Policy effectiveness, including:

- Number of breaches reported, investigated, and resolved;
- Frequency and outcomes of audits of access controls;

- Participation and completion rates for training;
- Compliance with document handling and retention procedures;
- Timeliness of review and amendment processes;
- Effectiveness of whistleblower protections and response times.

6.2. Metrics shall be reviewed by the NEC, Integrity Committee, and Legal Affairs Directorate, and findings incorporated into **annual NEC performance reports**.

## 7. Continuous Improvement

7.1. AAAIC shall adopt a **continuous improvement approach**, ensuring the NDA Policy evolves with:

- Organisational growth and structural changes;
- Emerging threats to information security;
- Technological advancements in data storage, communication, and encryption;
- Feedback from members, committees, and external stakeholders.

7.2. Recommendations for improvement shall be documented, assessed for feasibility, and, where approved, **integrated into the next policy iteration**.

## 8. Communication of Amendments

8.1. All approved amendments shall be **communicated formally**:

- Distribution via email, official portals, and committee channels;
- Highlighted in annual review bulletins;
- Accompanied by a summary of changes and implications for members.

8.2. Members must **acknowledge receipt** and understanding of the updated Policy, with non-compliance potentially affecting access to confidential information or participation in committees.

## 9. Accountability and Oversight

9.1. Oversight mechanisms include:

(a) NEC review of compliance reports;
(b) Integrity Committee audits of breach investigations and whistleblower protections;
(c) Legal review of Policy alignment with statutory obligations;
(d) Secretariat oversight of version control, distribution, and record-keeping.

9.2. Failure of officers or committees to implement, monitor, or enforce the NDA Policy constitutes a **policy violation** and may trigger corrective action or sanctions.

## 10. Integration with AAAIC Governance

10.1. This Part integrates with the broader governance and ethical framework of AAAIC, including:

- Constitution and Codes of Conduct;
- NDAs and contractual obligations;
- Risk management, compliance, and operational directives;
- Strategic and operational planning processes.

10.2. Implementation of the NDA Policy shall be treated as **a core component of organisational governance**, ensuring that confidentiality, integrity, and accountability are upheld at all levels.

## 11. Policy Lifecycle and Version Control

11.1. Each version of the NDA Policy shall include:

- Version number and date of issue;
- Summary of changes from prior version;
- Authorising signatures of NEC Chairperson and Secretary-General;
- Record of circulation and acknowledgment by members.

11.2. Superseded versions shall be **archived securely** for audit and legal purposes.

11.3. Version control ensures **clarity, traceability, and compliance** with both internal and external regulatory requirements.

**AAAIC NDA POLICY**

**ANNEXURES AND SCHEDULES**

**Annexure A**

**NDA Acknowledgement Form**

**Purpose:** To formally document that members, officials, staff, contractors, and partners have read, understood, and agreed to comply with AAAIC's NDA Policy.

| Field | Description |
|---|---|
| Name of Individual | Full legal name |
| Identity Number / Contractor Number | National ID or organisational ID |
| Position / Role | E.g., NEC member, committee official, contractor |
| Tier / Committee | Specify branch, REC/PEC, or department |
| Date of Acknowledgement | Date form is signed |
| Declaration | "I acknowledge that I have read, understood, and agree to comply with AAAIC's NDA Policy. I understand the obligations, penalties for breach, and reporting procedures." |
| Signature | Signed by individual |
| Witness / HR Officer | Signature of witness / policy officer |

**Instructions:**

- Must be completed prior to granting access to confidential information.
- Digital signatures acceptable with secure verification.
- Retain in individual personnel files for audit purposes.

**Annexure B**

**Confidential Information Handling Checklist**

**Purpose:** To provide step-by-step guidance for handling classified information in physical and digital form.

| Task | Yes / No | Notes / Responsible Party |
|---|---|---|
| Identify information classification (Confidential / Restricted / Secret / Public) | | |
| Ensure secure storage (locked cabinets, encrypted drives) | | |
| Limit access to authorised personnel only | | |
| Use approved communication channels for sharing | | |
| Avoid discussing confidential information in public or unsecured environments | | |
| Confirm removal / destruction of obsolete confidential documents | | |
| Report suspected mishandling immediately | | |
| Maintain access logs for digital files | | |
| Follow encryption standards for emails and digital storage | | |

**Instructions:**

- To be completed whenever new confidential material is issued or transmitted.
- Review monthly during compliance audits.

**Annexure C**

**Access Control Log Template**

**Purpose:** To record and track who accesses confidential, restricted, and secret information.

| Date | Name of Individual | Position / Role | Information Accessed | Purpose | Authorised By | Time In | Time Out | Notes |
|---|---|---|---|---|---|---|---|---|

**Instructions:**

- Maintain separate logs for physical and digital access.
- Authorisation must come from Confidentiality Compliance Officer or NEC-approved authority.
- Retain logs for **minimum of five years** or as per legal requirements.

**Annexure D**

**Breach Reporting Form**

**Purpose:** To report suspected breaches of the NDA Policy.

| Field | Description |
|---|---|
| Date of Report | |
| Reporting Individual | Name and role (optional if anonymous) |
| Contact Information | Phone, email, or secure portal ID |
| Alleged Offender | Name, role, and tier |
| Nature of Breach | Detailed description of actions or omissions |
| Classification of Information | Confidential / Restricted / Secret / Public |
| Evidence Provided | Attachments, screenshots, documents |
| Immediate Corrective Actions Taken | Steps already undertaken |

| Field | Description |
|---|---|
| Reporting Channel | Compliance Officer / Integrity Committee / Legal Directorate |
| Signature / Digital Verification | |

**Instructions:**

- Submit within **24 hours** of becoming aware of a suspected breach.
- Whistleblower protections automatically apply.

**Annexure E**

**Investigation Checklist**

**Purpose:** To ensure consistent, thorough investigation of NDA breaches.

| Step | Completed (Yes / No) | Notes / Responsible Officer |
|---|---|---|
| Preliminary assessment of report | | |
| Notification to alleged offender | | |
| Collection of evidence | | |
| Interviews conducted | | |
| Preservation of digital / physical evidence | | |
| Drafting investigative report | | |
| Review by Integrity Committee | | |
| Submission to NEC for adjudication | | |
| Communication of outcome to involved parties | | |
| Record retention and archiving | | |

**Annexure F — Sanction & Adjudication Record**

| Breach ID | Individual | Classification of Breach | Investigating Officer | Date Investigation Completed | NEC Decision | Sanction Applied | Appeal Status | Notes |
|---|---|---|---|---|---|---|---|---|

**Instructions:**

- Maintain confidentiality in all records.
- Ensure documentation aligns with version control and review timelines.

**Annexure G**

**Whistleblower Protection Acknowledgement**

**Purpose:** To confirm awareness of whistleblower rights and protections under AAAIC Policy.

| Field | Description |
|---|---|
| Name of Individual | |
| Role / Tier | |
| Date | |
| Declaration | “I understand that AAAIC protects whistleblowers who report in good faith. I acknowledge my rights, reporting channels, and protections against retaliation.” |
| Signature | |
| Witness / Compliance Officer | |

**Annexure H**

**Training Module Outline**

**Purpose:** To guide structured induction and refresher training for NDA compliance.

**Module 1:** Introduction to NDA Policy

- Purpose and rationale
- Legal and ethical foundations

**Module 2:** Definitions and Key Concepts

- Confidential, Restricted, Secret, Public
- Breach, Disclosure, Insider, Whistleblower

**Module 3:** Obligations and Behavioural Standards

- Duties of members, officials, contractors
- Handling and storage protocols

**Module 4:** Breach Enforcement

- Reporting, investigation, sanctions
- Interim measures and escalation

**Module 5:** Whistleblower Protections

- Reporting channels
- Retaliation safeguards

**Module 6:** Review and Policy Updates

- Annual review cycle
- Amendment and acknowledgement processes

**Module 7:** Practical Exercises & Case Studies

- Simulated breach scenarios
- Reporting exercises
- Corrective action planning

**Evaluation:**

- Quizzes, signed acknowledgement, scenario assessment, completion certificates.

**Annexure I — Digital & Physical Security Checklist**

| Task | Frequency | Responsible Officer | Notes |
|---|---|---|---|
| Password policy compliance | Monthly | IT / Compliance | Minimum 12-character encryption |
| Encryption verification | Monthly | IT | Email, drives, cloud storage |
| Access audit | Quarterly | Compliance Officer | Physical and digital access logs |
| Destruction of obsolete documents | Monthly | Department Head | Shredding or secure deletion |
| Backups and disaster recovery test | Quarterly | IT / Compliance | Verification of encrypted backups |

**Annexure J**

**Policy Review and Amendment Log**

| Version | Date | Summary of Changes | Approved By | Distribution Notes | Next Review Date |
|---|---|---|---|---|---|

**Instructions:**

- Maintain current version in central repository.
- Distribute updated copies to all tiers of AAAIC.
- Track acknowledgements by members and staff.

These **Annexures and Schedules**, when combined with Parts I–IX, will:

- Provide **operational guidance**;
- Ensure **legal and ethical compliance**;
- Standardise **reporting, investigation, and training processes**;
- Create a **fully auditable, over 100-page NDA Policy manual** suitable for NEC adoption.