# DRAFTING NOTE

NATIONAL INTELLIGENCE SERVICES ACT 2026

## 1. Status and purpose of this note

This drafting note is explanatory and is not part of the proposed Assembly Act. It identifies the legislative need, the relationship with earlier Eritrean law, the principal matters retained, the modernization choices made and the place of the draft within the emerging constitutional statute book. The instrument remains a consultation draft and should be finalized only after legal, institutional, fiscal and public review.

## 2. Legislative need and prior law

The supplied corpus does not provide a constitutionally adequate public statute for national intelligence. Secret power without a clear mandate, warrants, records and external oversight is incompatible with democratic government.

## 3. What the draft retains

The draft retains collection and analysis necessary to protect Eritrea against genuine external, violent and strategic threats.

## 4. What the draft updates and modernizes

It strictly separates intelligence from political policing, requires legality and necessity, judicial authorization for intrusive methods, minimization and data controls, legislative and independent oversight, financial audit, complaint and whistleblower protection, and classified but reviewable accountability.

## 5. Constitutional, code and treaty fit

The draft is framed under the Constitution of Eritrea 1997 and must be read with the Civil Code, Penal Code, Civil Procedure Code and Criminal Procedure Code of Eritrea 2015 where those Codes govern. It is also coordinated with the other institutional, financial, commercial, land, labour, administrative and sectoral drafts in this collection. References to international or regional standards guide compatibility and implementation; they do not bypass the Treaty-Making Act or convert an unincorporated instrument into domestic law.

## 6. Scope and organization

The principal divisions address preliminary and constitutional provisions; the national intelligence system; mandates, threats and prohibitions; personnel, professionalism and conduct; intelligence collection and sources; judicial warrants and intrusive powers; information, analysis and technology; cooperation and external relations; inspector-general of intelligence; legislative, judicial and financial oversight; and the concluding enforcement, transitional and final provisions.

## 7. Transition, implementation and consultation

The draft preserves lawful accrued rights, completed transactions, pending proceedings and institutional continuity where appropriate, while preventing temporary savings from preserving unconstitutional coercion or indefinite executive discretion. Before enactment or issuance, authentic predecessor instruments and amendments should be verified, cross-references and fiscal capacity confirmed, implementing regulations and digital systems prepared, and affected institutions, professions, communities and the public given a practical opportunity to comment.

CONSULTATION DRAFT — NOT ENACTED LAW

ACT NO. ___ OF 2026

# NATIONAL INTELLIGENCE SERVICES ACT 2026

(ASSEMBLY ACT)

AN ACT TO ESTABLISH A PROFESSIONAL, CIVILIAN AND POLITICALLY NEUTRAL NATIONAL INTELLIGENCE SERVICE; DEFINE AND LIMIT NATIONAL INTELLIGENCE MANDATES AND POWERS; REGULATE INTELLIGENCE COLLECTION, ANALYSIS, WARRANTS, INFORMATION, TECHNOLOGY, COOPERATION, PERSONNEL, FINANCE AND SECRECY; PROVIDE INDEPENDENT JUDICIAL, LEGISLATIVE, AUDIT AND INSPECTOR-GENERAL OVERSIGHT, COMPLAINTS AND REMEDIES; PROHIBIT POLITICAL SURVEILLANCE, SECRET DETENTION, TORTURE, DISAPPEARANCE, INDISCRIMINATE SURVEILLANCE AND UNAUTHORIZED COVERT ACTION; COORDINATE THE LAWFUL INTELLIGENCE FUNCTIONS OF PUBLIC INSTITUTIONS; AND PROVIDE FOR RELATED MATTERS.

## PREAMBLE

WHEREAS Articles 15 to 19, 24, 26, 28, 29, 32, 42, 49, 50 and 55 of the Constitution of Eritrea protect life, liberty, dignity, fair process, privacy, expression, administrative justice, enforceable rights, legislative supremacy, lawful executive government, independent courts and public audit;

WHEREAS Eritrea requires timely and reliable intelligence to protect its people, constitutional order, territorial integrity and peaceful relations, but intelligence institutions must never again become instruments of secret detention, disappearance, political fear, compulsory conformity or government without law;

WHEREAS secrecy may protect a lawful operation, source or method but shall not conceal illegality, corruption, human-rights abuse, unauthorized expenditure or institutional failure;

WHEREAS modern communications, artificial intelligence, biometrics, cyber operations and large datasets create both security capability and exceptional danger to liberty and democratic life, requiring specific law, necessity, proportionality, minimization, judicial authorization and independent review;

WHEREAS comparative democratic experience supports a clear statutory mandate, separation from policing and the military, executive responsibility, legislative scrutiny, judicial control of intrusive powers, unrestricted expert review and complete audit of public money;

NOW, THEREFORE, the National Assembly of Eritrea, acting under Articles 26 and 32 of the Constitution, enacts as follows:

## CHAPTER I
## PRELIMINARY AND CONSTITUTIONAL PROVISIONS

**Article 1 — Short title**

This Act may be cited as the "National Intelligence Services Act 2026".

**Article 2 — Objects**

1. to provide lawful intelligence capability against defined serious threats to Eritrea and its people;
2. to ensure that intelligence collection, analysis and advice are accurate, necessary, proportionate and politically neutral;
3. to place intrusive powers, secrecy, data, expenditure and cooperation under independent control and effective remedy; and
4. to dismantle and prevent secret, partisan, military, commercial or coercive intelligence government.

**Article 3 — Supremacy of the Constitution**

1. Every intelligence institution, official, operation, agreement, order and record is subject to the Constitution and Assembly Acts.
2. National security is a public responsibility under law and is not the personal interest of a President, party, commander, official or institution.
3. A classified, oral, foreign or executive direction cannot authorize conduct prohibited by the Constitution or this Act.
4. An official shall refuse and report a manifestly unlawful order and is protected for doing so.

**Article 4 — Application**

1. This Act applies to the National Intelligence Service and to every public body when performing a national-security or intelligence function.
2. Defence intelligence remains governed principally by the Defence Forces Act and criminal intelligence by the Police Service Act, subject to common safeguards expressly stated here.
3. It applies to intelligence obtained by a contractor, foreign partner, communications provider, artificial-intelligence system or other intermediary on behalf of Eritrea.
4. No institution may avoid this Act by changing the name, location, budget, technology or administrative sponsor of an intelligence activity.

**Article 5 — Interpretation**

1. "Service" means the National Intelligence Service established by Article 13;
2. "intelligence" means evaluated information reasonably relevant to a threat or opportunity within a statutory national-intelligence mandate;

3. “intrusive power” means covert interception, device access, entry, tracking, surveillance, source operation or acquisition creating comparable serious interference; and
4. “threat” means conduct within Article 33 and excludes lawful exercise of constitutional rights.

**Article 6 — Further definitions**

1. “bulk dataset” means a large collection containing personal information about persons most of whom are not suspected of a threat;
2. “content” means the substance or meaning of a communication, excluding narrowly defined communications data;
3. “Inspector-General” means the Inspector-General of Intelligence established by Article 122; and
4. “warrant” means prior written judicial authorization issued under Chapter VI.

**Article 7 — Guiding principles**

1. Intelligence activity shall have a specific lawful purpose, rational factual basis and defined responsibility.
2. Collection shall be necessary, proportionate, targeted and conducted through the least intrusive reasonably effective means.
3. Analysis shall distinguish fact, corroboration, assumption, uncertainty, dissent and policy preference.
4. Oversight shall be continuous, adequately resourced, independent and able to examine highly classified information without Service permission.

**Article 8 — Rights and lawful limitation**

1. A limitation of a right requires clear law and compliance with Article 26 of the Constitution.
2. Necessity shall be established by evidence of a legitimate threat, not by general assertion or institutional convenience.
3. Proportionality shall compare expected security value, seriousness and likelihood of harm, intrusion, alternatives, safeguards and duration.
4. The burden of justifying secret intrusive action rests on the authority seeking it.

**Article 9 — Prohibited discrimination**

1. Intelligence shall not target or disadvantage a person because of ethnicity, language, sex, gender, religion, region, disability, nationality, birth, wealth or another protected status.
2. Identity may be considered only where objectively and specifically relevant to a defined threat and never as a substitute for individualized grounds.
3. Analytic systems and datasets shall be tested for unlawful bias and unequal error.
4. A discriminatory direction, watchlist or profile shall be corrected, deleted and investigated.

**Article 10 — International law**

1. Intelligence activity shall respect a treaty lawfully binding on Eritrea and applicable international human-rights, humanitarian and refugee law.
2. No foreign request, agreement or assurance authorizes torture, refoulement, disappearance, unlawful detention or arbitrary surveillance.
3. An international arrangement shall comply with the Treaty-Making Act and may not confer domestic coercive power through executive consent alone.
4. A person under Eritrean authority or effective control receives applicable protection regardless of location or nationality.

**Article 11 — Relationship with other laws**

1. The Criminal Procedure Code and Courts Act govern warrants, evidence, judicial process and remedies except where this Act provides a stricter safeguard.
2. The Data Protection and Privacy Act governs intelligence processing except to the precise extent this Act establishes a necessary and independently supervised rule.
3. The Defence Forces, Police Service, Media Freedom, Access to Information, Public Finance, Procurement and public-integrity Acts remain applicable according to their purposes.
4. A conflict shall be resolved in favour of the Constitution and the more specific protection against intelligence abuse.

**Article 12 — No implied power**

1. An intelligence power exists only where this Act or another Assembly Act states it clearly.
2. Administrative necessity, custom, classification, technology, foreign practice or prior use does not create power.
3. A regulation, policy, warrant or agreement may narrow but shall not enlarge a statutory power.
4. Uncertainty about authority shall be resolved before collection begins through legal advice or judicial determination.

## CHAPTER II
## THE NATIONAL INTELLIGENCE SYSTEM

**Article 13 — Establishment of the Service**

1. The National Intelligence Service is established as a civilian executive institution with legal personality and national jurisdiction.
2. It is separate from the Defence Forces, Police Service, prosecution service, political organizations and private security providers.
3. Its headquarters shall be in Asmara, and another office may be established only for an identified operational need and recorded authorization.
4. The Service may sue and be sued, contract and hold property only for its statutory functions.

**Article 14 — Civilian and politically neutral character**

1. The Service shall be civilian in leadership, organization, training, appearance and operational culture.
2. It shall serve the Constitution and elected institutions regardless of political composition.
3. No officer shall hold active party office, campaign, direct political financing or use intelligence to influence an election or legislative vote.
4. Political loyalty, liberation history, military rank, ethnicity, region or family connection is not a qualification for intelligence service.

**Article 15 — Principal functions**

1. The Service shall collect, evaluate and report foreign and domestic security intelligence within the defined mandates of this Act.
2. It shall conduct lawful counter-intelligence, security assessment and protective intelligence for constitutional institutions and critical assets.
3. It shall provide objective strategic warning and national assessments to authorized decision-makers.
4. It shall not make policy, administer ordinary government, enforce law or determine guilt.

**Article 16 — Absence of law-enforcement powers**

1. The Service has no power to arrest, detain, imprison, punish, prosecute, compel testimony, impose a fine or operate a detention place.
2. It may not execute a police search or seizure, control a prison, maintain an armed tactical unit or direct a criminal investigation.
3. Where intelligence indicates crime, the Service shall refer information lawfully to the Police Service or prosecutor.
4. A police officer seconded to the Service shall not exercise police power under Service command.

**Article 17 — No military command**

1. The Service shall not command Defence Forces personnel, units, weapons, bases or operations.
2. Defence intelligence shall not command the Service or conduct domestic civilian surveillance through military authority.
3. Joint work requires written lead responsibility, legal authority and oversight access.
4. A security emergency does not merge intelligence, police and military institutions except under a specific lawful temporary arrangement.

**Article 18 — Responsible minister**

1. The President shall designate by published executive regulation a minister responsible for democratic executive oversight of the Service.

2. The minister shall approve general priorities, ensure legality and resources and answer to the National Assembly.
3. The minister shall not direct an assessment conclusion, target a person for political or private purpose or bypass a warrant.
4. A material ministerial direction shall be written, legally reviewed, retained and available to oversight bodies.

**Article 19 — Presidential and Cabinet responsibility**

1. The President and Cabinet may establish lawful national-security priorities and receive intelligence necessary for constitutional functions.
2. They shall not create a secret intelligence institution, unappropriated fund, detention power or surveillance programme.
3. A presidential request concerning an identifiable person shall state a lawful threat-related purpose and be recorded for Inspector-General review.
4. Intelligence shall not be supplied for personal, party, commercial, electoral or retaliatory use.

**Article 20 — Director-General**

1. The President shall appoint the Director-General from a public merit shortlist with approval of the National Assembly.
2. The Director-General serves one six-year term and shall possess integrity, senior leadership, legal understanding and intelligence or comparable security expertise.
3. The Director-General is the accounting officer, controls lawful operations and is responsible for compliance and truthful reporting.
4. Appointment, qualifications and declared interests shall be published without disclosing protected operational information.

**Article 21 — Ineligibility for Director-General**

1. A serving political-party officer, elected official, active member of the Defence Forces or controlling government contractor is ineligible.
2. A person credibly implicated in torture, disappearance, secret detention, political persecution, corruption or destruction of public records shall not be appointed pending independent resolution.
3. Prior government, military or liberation service is neither automatic qualification nor automatic disqualification.
4. The appointment process shall examine individual conduct, competence, conflicts and commitment to constitutional government.

**Article 22 — Removal of Director-General**

1. The Director-General may be removed for incapacity, serious misconduct, grave illegality, corruption, material deception of oversight bodies or persistent failure of duty.

2. Removal requires stated allegations, access to evidence, fair response and independent inquiry.
3. The President may suspend temporarily to protect an inquiry but shall notify the National Assembly and Inspector-General immediately.
4. Final removal requires National Assembly approval and published reasons subject to protection of strictly operational detail.

**Article 23 — Deputy Directors-General**

1. The Service shall have Deputy Directors-General for foreign intelligence, security intelligence, analysis and lawful technical support.
2. The Director-General shall appoint them through open merit process subject to security vetting and Board-level integrity review prescribed by regulation.
3. Collection and final all-source assessment shall be organizationally separated to protect analytic independence.
4. A deputy shall not operate a personal, ethnic, military, party or regional chain of command.

**Article 24 — Foreign Intelligence Directorate**

1. The Foreign Intelligence Directorate shall collect and analyze information concerning external threats and strategic developments relevant to Eritrea.
2. It shall prioritize territorial integrity, regional stability, foreign military activity, transnational threats, diplomacy, technology and economic security.
3. It shall not interfere unlawfully in a foreign political process or conduct violence, sabotage, kidnapping or destabilization.
4. Activity affecting a person in Eritrea or an Eritrean-controlled system remains subject to domestic warrant safeguards.

**Article 25 — Security Intelligence Directorate**

1. The Security Intelligence Directorate shall assess espionage, terrorism, sabotage, violent subversion and comparable threats within Eritrea.
2. Its mandate is preventive intelligence and counter-intelligence, not ordinary crime, political opposition or social control.
3. Domestic collection requires specific grounds connecting a person, place or activity to a statutory threat.
4. It shall cooperate with police through lawful referral without controlling arrest, charging or prosecution.

**Article 26 — Analysis Directorate**

1. The Analysis Directorate shall produce independent all-source assessments for authorized constitutional decision-makers.
2. It shall state sourcing, reliability, gaps, alternatives, probability, dissent and consequences of error.

3. Policy officials may request questions and clarify assumptions but shall not dictate findings.
4. Material politicization or suppression of analysis shall be recorded and reported to the Inspector-General.

**Article 27 — Technical Support Directorate**

1. The Technical Support Directorate shall provide secure communications, cyber defence, forensic, data and warrant-execution capability within law.
2. It shall not create an independent collection mandate or operate a system without an identified legal owner and purpose.
3. System architecture shall enforce authorization, minimization, access control, logging, retention and oversight access.
4. A capability designed to evade law, conceal access or disable audit is prohibited.

**Article 28 — National Intelligence Coordination Council**

1. A National Intelligence Coordination Council is established to coordinate lawful intelligence among the Service, Defence Forces, Police Service, border institutions and other authorized bodies.
2. The Council shall resolve duplication, agree threat definitions, coordinate assessments and ensure referral to the institution with lawful authority.
3. It shall not collect intelligence, issue warrants, direct police or military operations or create a joint secret force.
4. Its membership, decisions and tasking shall be recorded and available to oversight bodies.

**Article 29 — National intelligence priorities**

1. The Cabinet shall approve annual national intelligence priorities proposed by the responsible minister after legal and threat assessment.
2. Priorities shall identify statutory threats, questions, responsible institutions, resource implications and excluded activities.
3. The classified priorities shall be provided in full to the Inspector-General and appropriate National Assembly committee.
4. A public summary shall explain principal threat categories without exposing a lawful operation or person.

**Article 30 — Tasking and consumers**

1. Intelligence may be tasked and received only by offices identified in law, national priorities or an authorized operational record.
2. A request shall state the decision need and shall not ask the Service to collect political, personal or commercial advantage.
3. Dissemination shall be limited to persons with lawful need and recorded accountability.
4. The Service shall correct a material error supplied to every known recipient promptly.

**Article 31 — Professional legal office**

1. The Service shall maintain an independent professional legal office led by counsel appointed on merit.
2. Counsel shall review intrusive applications, agreements, novel capabilities, ministerial directions, serious incidents and proposed public rules.
3. Legal advice shall not be manipulated, withheld from oversight or used to create artificial immunity.
4. Counsel may report an unresolved serious legality concern directly to the Director-General and Inspector-General.

**Article 32 — Public liaison and service**

1. The Service shall maintain public contact for lawful reporting, complaints, employment information and published institutional material.
2. A person shall not be compelled to become a source merely because the person seeks a passport, licence, job, education, benefit or other public service.
3. Diaspora contact, consular use or return to Eritrea is not by itself an intelligence ground.
4. Public outreach shall not become propaganda, political recruitment or concealed collection.

## CHAPTER III
## MANDATES, THREATS AND PROHIBITIONS

**Article 33 — Defined threats**

1. A threat within the Service mandate is espionage, terrorism, sabotage, violent overthrow of the constitutional order or serious foreign interference.
2. It includes proliferation of weapons of mass destruction, hostile cyber operation against critical systems and transnational organized conduct presenting comparable national harm.
3. It may include a specific imminent threat to territorial integrity, constitutional institutions or essential national infrastructure.
4. It does not include lawful advocacy, protest, reporting, religion, association, migration, labour activity or criticism.

**Article 34 — Espionage and foreign interference**

1. Espionage means clandestine acquisition or disclosure of protected national-security information for a foreign power or comparable hostile actor.
2. Foreign interference means covert, deceptive, coercive or corrupt foreign direction intended seriously to impair constitutional decision-making or rights.
3. Open diplomacy, journalism, scholarship, trade, cultural exchange and diaspora engagement are not interference without additional threatening conduct.
4. Countermeasures shall be lawful, evidence-based and proportionate and shall protect legitimate international contact.

**Article 35 — Terrorism**

1. Terrorism requires serious violence, hostage-taking or comparable grave danger intended to intimidate a population or compel government for political, ideological or religious purpose.
2. Peaceful civil disobedience, strike, protest, advocacy and political opposition are not terrorism.
3. The label shall not be applied by ethnicity, religion, region, exile status or association alone.
4. Intelligence assessment does not determine criminal liability and shall distinguish suspicion from proof.

**Article 36 — Sabotage and violent subversion**

1. Sabotage means intentional serious damage to defence, essential infrastructure or critical systems for a hostile strategic purpose.
2. Violent subversion means organized use or preparation of serious violence to overthrow or disable the constitutional order.
3. Advocacy of constitutional change, replacement of government, federal arrangement, independence history or another political position is not subversion without violent conduct.
4. The Service shall not investigate ideology as a substitute for evidence of a statutory threat.

**Article 37 — Economic and resource security**

1. The Service may assess hostile corruption, illicit influence, strategic coercion, proliferation financing and attacks on critical economic systems.
2. It shall not investigate ordinary market competition, tax dispute, labour organization or criticism of economic policy as national-security threats.
3. Commercial intelligence shall not be supplied to a State-owned or private enterprise for competitive advantage.
4. Suspected financial crime shall be referred to the competent regulator, police or prosecutor.

**Article 38 — Protective intelligence**

1. The Service may assess specific threats to constitutional officeholders, visiting dignitaries and designated critical institutions.
2. Protection shall be coordinated with the Police Service and Defence Forces according to lawful functions.
3. Protective intelligence shall not monitor political opponents, protesters, journalists or ordinary visitors without threat-based grounds.
4. A protectee shall not direct collection for personal or political purpose.

**Article 39 — Security assessments**

1. A security assessment may be conducted for access to clearly identified classified information, sensitive systems or exceptional national-security office.
2. Assessment shall be relevant, individualized, accurate, time-limited and subject to response and review to the greatest extent compatible with source protection.
3. Political opinion, lawful association, family origin, religion, foreign residence or criticism shall not alone justify adverse assessment.
4. A general civil-service, education, business or travel opportunity shall not require intelligence clearance.

**Article 40 — No political intelligence**

1. The Service shall not collect, analyze, retain or disseminate information for monitoring lawful political opinion, parties, candidates, legislators, voters or campaigns.
2. It shall not influence an election, nomination, legislative vote, judicial appointment, media debate or peaceful transition of government.
3. No government or opposition figure may receive secret intelligence assistance against a political rival.
4. Incidental political information unrelated to a threat shall be deleted and not disseminated.

**Article 41 — No surveillance of protected civic activity**

1. Journalism, source contact, legal representation, worship, union activity, academic inquiry, human-rights work and peaceful assembly receive heightened protection.
2. Participation in such activity does not establish reasonable grounds for collection.
3. Collection that unavoidably affects a protected function requires heightened necessity, minimization and warrant safeguards.
4. The Inspector-General shall review every operation materially affecting a protected civic function.

**Article 42 — Prohibition of detention and disappearance**

1. The Service shall not operate, finance, request, conceal or assist a secret or unauthorized detention place.
2. An officer shall not arrest, abduct, transfer, disappear or hold a person for questioning.
3. Contact with a person shall be voluntary unless a court or lawful police authority acts under another Act.
4. Knowledge of unlawful detention or disappearance shall be reported immediately to the court, prosecutor and Inspector-General.

**Article 43 — Prohibition of torture and cruel treatment**

1. Torture and cruel, inhuman or degrading treatment or punishment are absolutely prohibited without exception.

2. The Service shall not request, encourage, finance, participate in or conceal such treatment by another person or State.
3. Information known to have been obtained through torture shall not be used except to protect a person or investigate the abuse, with clear warning of unreliability.
4. A diplomatic assurance shall not justify transfer where substantial risk of prohibited treatment remains.

**Article 44 — Prohibition of assassination and unauthorized force**

1. The Service shall not kill, wound, kidnap, render or use force except ordinary necessary self-defence available to any person under law.
2. It shall not maintain weapons beyond narrowly licensed personal protection appropriate to demonstrated risk.
3. No executive order may authorize assassination, punishment or lethal covert action.
4. An external use of armed force is governed by the Constitution, Defence Forces Act and international law, not this Act.

**Article 45 — Prohibition of covert political action**

1. The Service shall not secretly fund, direct, infiltrate or manipulate an Eritrean party, campaign, media outlet, religious body, union, association or protest.
2. It shall not fabricate evidence, spread disinformation, manufacture public support or organize a front body for domestic political effect.
3. A foreign covert influence operation may be investigated but shall be countered through lawful attributed measures wherever practicable.
4. Public communication by the Service shall be accurate, authorized and distinguish fact from assessment.

**Article 46 — Prohibition of commercial activity**

1. The Service shall not own or control a commercial enterprise, mining interest, farm, transport business, media outlet, bank account network or trading operation.
2. A narrowly necessary operational cover arrangement requires warrant-level approval, complete financial record and Inspector-General access and shall not conduct substantial commerce.
3. Intelligence funds shall not finance personal enrichment, political organization or off-budget development.
4. Legacy commercial interests shall be disclosed, secured and transferred or liquidated lawfully under Chapter XIII.

**Article 47 — No coercive informant recruitment**

1. A person shall not be threatened with detention, prosecution, national service, passport denial, property loss or harm to family to compel cooperation.
2. A public benefit, immigration process, employment or licence shall not be conditioned on secret reporting absent a general legal duty applicable to all.

3. A source relationship shall be voluntary, documented, supervised and terminable, subject to protection of lawful obligations.
4. A child or vulnerable person may be used as a source only in an exceptional life-protection case with judicial authorization and independent safeguards.

**Article 48 — Duty to report imminent harm**

1. The Service shall communicate credible intelligence of imminent serious harm promptly to the institution able lawfully to prevent it.
2. Referral shall include reliability, urgency, limitations and handling requirements.
3. Source protection shall be balanced against life and fair-process duties through judicial procedure where necessary.
4. Failure to report for political, personal or institutional advantage is serious misconduct.

## CHAPTER IV
## PERSONNEL, PROFESSIONALISM AND CONDUCT

**Article 49 — Merit-based service**

1. Service personnel shall be recruited and promoted through fair merit procedures based on competence, integrity and operational need.
2. Recruitment shall seek gender, linguistic, regional and professional breadth without ethnic, religious or political allocation.
3. No secret patronage list, family preference, military quota or party sponsorship is permitted.
4. Appointments and establishments shall be authorized, recorded and financed through lawful public-employment systems adapted to necessary secrecy.

**Article 50 — Civil Service Administration Act**

1. Personnel are public servants governed by the Civil Service Administration Act except for specific security arrangements lawfully prescribed under this Act.
2. A security exception shall be necessary, proportionate and shall not remove fair pay, leave, health, pension, discipline, grievance or remedy.
3. The Civil Service Administration Commission may inspect general employment systems while protecting operational identities.
4. Intelligence classification shall not conceal payroll ghosts, discrimination, unpaid labour or arbitrary dismissal.

**Article 51 — Security vetting**

1. Vetting shall assess honesty, reliability, vulnerability, conflicts, serious misconduct and ability to protect information.
2. It shall use consent and lawful data, verify adverse information and avoid irrelevant intrusion into beliefs, family and intimate life.

3. A materially adverse decision shall provide sufficient reasons and an independent appeal consistent with source protection.
4. Vetting shall be reviewed periodically and shall not become continuous political surveillance.

**Article 52 — Oath and constitutional duty**

1. Before duty, every officer shall swear or affirm loyalty to the Constitution and lawful institutions rather than to an individual or organization.
2. The oath shall include respect for rights, truth in analysis, lawful secrecy, refusal of unlawful orders and cooperation with oversight.
3. An oath does not excuse crime, concealment from authorized oversight or false evidence.
4. The text of the oath and code of conduct shall be public.

**Article 53 — Training**

1. Initial and continuing training shall cover the Constitution, statutory mandate, human rights, warrants, data, analysis, interviewing, ethics and oversight.
2. Specialized technical or source work requires certified competence and supervised practice.
3. Training shall examine Eritrea's history of secret coercion and methods of preventing institutional recurrence.
4. Completion, testing and remedial requirements shall be recorded and reviewed by the Inspector-General.

**Article 54 — Code of conduct**

1. The Director-General shall issue a public code of conduct after consultation with the Inspector-General and approval by the responsible minister.
2. The code shall govern legality, impartiality, conflicts, sources, gifts, information, force, public contact, reporting and post-service conduct.
3. It may impose professional discipline but shall not create an offence or intelligence power.
4. A secret supplement may address operational detail only and shall be available in full to oversight bodies.

**Article 55 — Conflict of interest**

1. An officer shall disclose financial, family, political, foreign, professional and other interests reasonably affecting duty.
2. A conflicted officer shall recuse, divest or accept another proportionate control directed by an authorized ethics official.
3. Information or influence shall not be used for personal investment, employment, family advantage or harm to a competitor.
4. Declarations and controls shall be auditable and significant breaches reported to the Inspector-General.

**Article 56 — Gifts and benefits**

1. An officer shall not solicit or accept a benefit that could influence, reward or appear to purchase intelligence action.
2. A foreign gift or hospitality shall be declared, valued and disposed of under public-service law.
3. Operational payments to a source require prior authorization, documentation, proportionality and independent financial review.
4. A payment shall not procure unlawful conduct or evidence known to be fabricated.

**Article 57 — Discipline**

1. Discipline shall address misconduct through written allegation, evidence, response, impartial decision and proportionate sanction.
2. Security-sensitive procedure may protect information but shall provide counsel and an effective means to answer the case.
3. An officer shall not be disciplined for lawful disclosure to an oversight body, refusal of unlawful order or protected reporting.
4. Criminal conduct shall be referred independently and shall not be resolved only by internal transfer or retirement.

**Article 58 — Grievances and association**

1. Personnel may raise employment, safety, ethics and legality grievances through secure and independent channels.
2. Lawful professional association and collective representation may be regulated only to protect operations and political neutrality, not abolished categorically.
3. A representative may assist an officer without receiving unrelated classified information.
4. Retaliation for a good-faith grievance is prohibited.

**Article 59 — Health and psychological support**

1. The Service shall provide occupational safety, medical and confidential psychological support appropriate to intelligence work.
2. Health information shall not be used for unrelated intelligence or retaliation and shall be accessed only as law permits.
3. Exposure to trauma, undercover stress and moral injury shall receive preventive and continuing care.
4. A fitness decision shall be professional, individualized, reviewable and accompanied by reasonable accommodation where possible.

**Article 60 — Weapons and protective equipment**

1. Only specifically designated and trained protection personnel may carry a licensed weapon for demonstrated personal or facility protection need.

2. Weapons, ammunition and tactical equipment shall be inventoried, secured, audited and never used for arrest, interrogation or intimidation.
3. Discharge or loss shall be reported immediately to police, the Inspector-General and responsible command.
4. The Service shall not procure weapons designed principally for torture, indiscriminate force or military combat.

**Article 61 — Former personnel**

1. Former personnel remain bound by lawful secrecy concerning protected operations, sources and personal information.
2. Secrecy does not prohibit reporting illegality to authorized bodies, complying with court process or making a protected public-interest disclosure under law.
3. Post-service employment and contact shall be governed by proportionate conflict and cooling-off rules.
4. Pension, records and lawful benefits shall not be withheld to enforce political silence.

**Article 62 — Identity and cover**

1. An operational identity or cover arrangement requires written purpose, duration, legal review, supervisory approval and protected records.
2. It shall not be used to commit fraud for private gain, enter an intimate relationship deceptively, vote, hold political office or evade court authority.
3. Civil documents created for lawful cover shall be controlled, reconciled and cancelled when no longer necessary.
4. A court and the Inspector-General may access true identity under secure procedure.

## CHAPTER V
## INTELLIGENCE COLLECTION AND SOURCES

**Article 63 — Collection plan**

1. Every collection activity shall have a written plan identifying mandate, threat, grounds, objectives, methods, duration, risk, minimization and supervision.
2. A plan shall distinguish open, consensual, covert and intrusive methods and identify any required warrant.
3. The approving officer shall test necessity, alternatives, expected value and effect on uninvolved persons.
4. Material change requires renewed approval before implementation except immediate life protection.

**Article 64 — Open-source intelligence**

1. The Service may collect lawfully public information for a defined statutory intelligence purpose.

2. Public availability does not remove privacy, data-protection, accuracy, retention and discrimination duties.
3. Systematic monitoring, identity resolution or large-scale aggregation may become intrusive and require enhanced authorization.
4. Lawful anonymous political or journalistic expression shall not be unmasked without warrant grounds tied to a threat.

**Article 65 — Voluntary information**

1. A person may provide information voluntarily after being informed of the Service identity and purpose unless lawful cover is necessary.
2. Consent shall not be manufactured through authority, deception about legal obligation or threat to a public service.
3. Information shall be assessed, recorded and minimized rather than accepted as verified fact.
4. The Service shall provide a secure means to report imminent threats and corruption within the Service.

**Article 66 — Human sources**

1. Recruitment and operation of a human source requires written assessment, voluntary agreement, risk plan, supervisor and periodic renewal.
2. A source shall not be authorized to incite an offence, entrap a person, use violence or interfere with constitutional activity.
3. Payment, benefit, reliability, motive, criminality and handling shall be documented and disclosed where fair process requires.
4. A source relationship affecting a lawyer, journalist, legislator, judge, religious leader or medical professional requires prior judicial authorization.

**Article 67 — Undercover activity**

1. Undercover contact requires necessity, proportionality, defined identity, target, conduct, duration and close supervision.
2. It shall not create an offence that would not otherwise occur or manipulate protected civic activity.
3. A sexual relationship, marriage, parenthood, medical role, legal representation or clergy role shall not be used as operational deception.
4. Material evidence of crime shall be preserved and referred without concealing exculpatory circumstances.

**Article 68 — Observation in public**

1. Limited observation in public may be authorized on specific grounds relevant to a threat.
2. Prolonged, covert, technologically enhanced or pattern-revealing observation requires a warrant.
3. Recording shall be minimized to relevant persons and events, with incidental data deleted.

4. A public gathering shall not be monitored solely to identify participants or opinions.

**Article 69 — Requests to public bodies**

1. The Service may request information from a public body only where statute permits the body to disclose it for the stated purpose.
2. The request shall identify authority, necessity, scope, retention and any warrant.
3. A public body shall not create a secret database, routine feed or exception from its governing Act by agreement alone.
4. Every disclosure shall be logged and available to the Inspector-General and data-protection authority.

**Article 70 — Requests to private persons**

1. A private person may disclose information voluntarily only as permitted by contract, privacy and sector law.
2. Compulsory production, interception, subscriber information or confidential records require statutory process and judicial authorization.
3. The Service shall not demand informal access by threatening licence, tax, immigration, procurement or regulatory consequences.
4. A provider may challenge a demand before a court and is protected for refusing an unlawful request.

**Article 71 — Financial intelligence**

1. The Service may receive intelligence lawfully disseminated by the financial-intelligence authority for a defined threat.
2. It shall not direct a financial institution to freeze, debit, close or disclose an account without the authority and process in the governing Act.
3. Financial data shall not be used to map political support, diaspora remittance or lawful association.
4. Suspicion, transaction context, lawful source and alternative explanation shall be assessed before dissemination.

**Article 72 — Travel and border intelligence**

1. Travel, passenger and border information may be used only under immigration, customs, aviation, maritime and data-protection law for a defined threat.
2. The Service shall not deny a passport, exit, entry or nationality decision and shall not maintain an unreviewable travel blacklist.
3. A recommendation to a competent authority shall identify grounds, reliability, duration and review status.
4. A person affected by an adverse travel measure shall receive reasons and remedy to the greatest lawful extent.

**Article 73 — Physical entry and search**

1. Covert entry onto private premises, installation of a device, search or taking of property requires a warrant.
2. The warrant shall specify place, purpose, authorized acts, property, duration, minimization and restoration.
3. Entry shall avoid damage and interference beyond what is necessary and shall not authorize detention or violence.
4. A complete inventory and execution report shall be filed securely with the issuing court.

**Article 74 — Communications interception**

1. Interception of communication content in transmission requires a targeted warrant under Chapter VI.
2. Acquisition of communications data, location or subscriber history requires judicial authorization proportionate to sensitivity and scope.
3. Indiscriminate or population-wide interception and generalized retention are prohibited.
4. A provider shall assist only to the extent stated by law and warrant and shall preserve security for other users.

**Article 75 — Equipment interference**

1. Remote or physical access to a device, account, network or software requires a specific equipment-interference warrant.
2. The application shall disclose vulnerabilities, collateral systems, data sought, security risk and deletion plan.
3. A systemic weakness, indiscriminate malware or continuing access beyond the target is prohibited.
4. A serious unpatched vulnerability affecting the public shall be reported through a lawful vulnerability-equities process.

**Article 76 — Location tracking**

1. Covert real-time or historical tracking of a person, device, vehicle or object requires a warrant except a narrow emergency under Article 93.
2. The application shall identify target, technology, accuracy, third-party effects, duration and minimization.
3. A tracking order shall not authorize entry, content access or continuous surveillance beyond its terms.
4. Data unrelated to the threat shall be deleted promptly.

**Article 77 — Biometrics and facial recognition**

1. Use of face, voice, gait, genetic or other biometric identification requires express statutory authority and a warrant where used covertly or at scale.
2. Real-time indiscriminate identification in public space is prohibited.

3. Systems shall be independently tested for accuracy, demographic error, security and necessity before use.
4. A match is investigative information, not proof, and requires accountable human verification.

**Article 78 — Bulk datasets**

1. The Service shall not acquire or retain a bulk dataset merely because it may become useful.
2. A necessary dataset with substantial information about uninvolved persons requires a special warrant, strict selection rules and periodic renewal.
3. The application shall describe provenance, scale, fields, affected persons, analytic use, error, safeguards, retention and alternatives.
4. Population-wide communications content, biometric or genetic databases for intelligence use are prohibited.

**Article 79 — Operational review**

1. The responsible supervisor shall review each ongoing covert or intrusive activity at intervals stated in authorization.
2. Review shall assess continued grounds, results, collateral intrusion, compliance, source conduct and whether less intrusive means now suffice.
3. An activity shall cease immediately when authority, necessity or proportionality ends.
4. Closure shall document results, incidents, deletion, notice and lessons.

## CHAPTER VI
## JUDICIAL WARRANTS AND INTRUSIVE POWERS

**Article 80 — Exclusive authority for intrusive powers**

1. An intrusive power may be exercised only under a warrant issued by an independent judge under this Chapter.
2. Executive approval, consent of a service provider, foreign request or classification does not substitute for a warrant.
3. A warrant authorizes only the persons, methods, information, premises and period stated.
4. Evidence obtained outside authority shall be secured, reported and not used except as a court permits to protect life or remedy illegality.

**Article 81 — Intelligence Warrants Chamber**

1. The Chief Justice, on recommendation of the Judicial Service Commission, shall designate at least five experienced judges to an Intelligence Warrants Chamber.
2. Designation shall be based on integrity, constitutional competence, technical understanding and independence for a fixed renewable period.
3. The executive and Service shall have no role in selecting or removing a designated judge.
4. The judiciary shall provide secure staff, records and technology under judicial control.

**Article 82 — Independence and duty of the judge**

1. A warrants judge shall test law, facts, necessity, proportionality, scope, safeguards and candour independently.
2. The judge may question applicants, require evidence, appoint independent counsel and refuse, narrow or condition a request.
3. National-security assertion and classification are relevant but not conclusive.
4. A judge shall report material deception, illegality or systemic concern to the Chief Justice and Inspector-General.

**Article 83 — Who may apply**

1. Only the Director-General or a Deputy Director-General specifically designated in writing may apply for a warrant.
2. The application requires prior legal-office review and certification of statutory authority.
3. The responsible minister shall approve an application for interception, equipment interference, bulk dataset or protected-function surveillance before judicial submission.
4. Ministerial approval does not bind the judge and shall not be delegated below minister during ordinary circumstances.

**Article 84 — Application requirements**

1. An application shall be written, sworn and identify applicant, target, threat, facts, purpose, methods, duration and information sought.
2. It shall disclose alternatives, collateral persons, protected functions, prior applications, known contrary facts, reliability and anticipated dissemination.
3. It shall propose minimization, retention, deletion, security, audit, notice and review conditions.
4. Material omission or misleading presentation breaches the duty of utmost candour.

**Article 85 — Grounds for issue**

1. The judge may issue a warrant only on probable cause that the target or facility is materially connected to a defined threat.
2. The authorized measure shall be necessary for a legitimate intelligence purpose and proportionate to seriousness, likelihood and intrusion.
3. Less intrusive reasonably effective methods shall be inadequate or materially riskier.
4. Safeguards shall make collateral collection, misuse, error and duration no greater than reasonably necessary.

**Article 86 — Particularity**

1. A warrant shall identify or describe with reasonable particularity the target, account, device, premises, communication, data or source category.

2. It shall state authorized methods, officers, assistance, execution period, reporting, minimization, retention and review.
3. A general warrant authorizing collection against an undefined class or any person associated with lawful activity is invalid.
4. Technical identifiers may supplement but shall not replace intelligible judicial description.

**Article 87 — Duration and renewal**

1. A targeted warrant may last no longer than ninety days, and a bulk-dataset warrant no longer than sixty days.
2. A shorter period shall be used where threat, intrusion or uncertainty warrants it.
3. Renewal requires a fresh application stating results, compliance, continued grounds, errors and alternatives.
4. Expiration ends collection immediately but does not determine lawful retention of previously acquired information.

**Article 88 — Protected functions**

1. A warrant affecting lawyer-client privilege, journalistic sources, a legislator, judge, clergy confession, medical confidentiality or electoral administration requires heightened necessity.
2. It shall be decided by a panel of three warrants judges and narrowly tailored to information not obtainable through less intrusive means.
3. Independent counsel shall test the application unless an immediate life-threatening emergency makes that impossible.
4. Privileged or protected material shall be segregated and accessed only under further judicial direction.

**Article 89 — Third-party and collateral information**

1. A warrant shall anticipate communications and information of persons not suspected of a threat.
2. Collection systems shall filter, segregate and delete collateral information as early as practicable.
3. Intentional examination of an unrelated person's protected information requires separate authority.
4. Material unforeseen intrusion shall be reported promptly to the judge and Inspector-General.

**Article 90 — Service-provider assistance**

1. A warrant may require a communications or technology provider to give specified reasonable assistance within its technical capability.
2. Assistance shall not require a systemic weakness, indiscriminate access, false public representation or continuing uncontrolled capability.
3. Reasonable verified direct cost shall be compensated through appropriated funds.

4. The provider may seek confidential judicial variation where compliance is impossible, unsafe or broader than authority.

**Article 91 — Execution report**

1. The executing officer shall file a secure return stating dates, methods, information obtained, incidents, collateral collection and compliance.
2. The return shall identify any departure, technical overcollection, protected material, damage or provider concern.
3. The judge may order cessation, deletion, segregation, notice, corrective action or further investigation.
4. The Inspector-General receives every application, warrant, refusal, variation, return and judicial direction automatically.

**Article 92 — Material error and excess**

1. Unauthorized collection, wrong targeting, excess scope, serious security breach or misleading application is a material error.
2. The Service shall stop affected activity, preserve evidence and notify the judge, minister and Inspector-General immediately.
3. Information shall be quarantined and not disseminated until a judicial direction determines treatment.
4. Corrective action shall address the affected person, system, officer, recipient and institutional cause.

**Article 93 — Emergency authorization**

1. Where an imminent threat to life or catastrophic harm makes prior judicial application impossible, the Director-General and responsible minister may jointly authorize a targeted measure.
2. The authorization shall state facts, method, scope, minimization and why delay was impossible and shall last no longer than twenty-four hours.
3. A warrants judge shall receive the full application as soon as practicable and no later than twelve hours after commencement.
4. If judicial approval is refused or narrowed, collection shall cease and information shall be deleted or treated as the judge directs.

**Article 94 — No emergency bulk power**

1. Emergency authority shall not permit indiscriminate interception, population database acquisition, generalized device interference or surveillance of a political group.
2. It shall not be used because ordinary preparation, staffing or judicial access was inadequate.
3. Repeated emergency use concerning the same threat is prohibited absent judicial finding of truly distinct circumstances.

4. Every emergency use shall be specifically reviewed and included in classified and public statistics.

**Article 95 — Variation and cancellation**

1. A material expansion of target, method, data, premises or duration requires judicial variation before effect.
2. The Service shall apply to cancel or narrow a warrant when grounds or necessity diminish.
3. A judge may vary, suspend or cancel on own initiative upon new information or noncompliance.
4. Cancellation shall trigger cessation, record preservation and a decision on retained information and notice.

**Article 96 — Notice after surveillance**

1. A person subjected to an intrusive power shall receive notice after secrecy is no longer strictly necessary to protect a specific operation, source or person.
2. Notice shall identify general measure, period, legal authority and route to complaint without revealing protected detail unnecessarily.
3. Continued deferral beyond three years requires annual judicial approval on evidence of current serious risk.
4. The Inspector-General may apply for earlier notice and shall report aggregate deferrals.

**Article 97 — Judicial records and public statistics**

1. The Chamber shall preserve complete secure records independent of the Service.
2. The Chief Justice shall publish annual aggregate numbers of applications, approvals, refusals, variations, emergencies, protected-function cases, errors and notices.
3. Statistics shall be sufficiently detailed to reveal trends while protecting lawful operations and individuals.
4. Judicial rules and significant redacted legal interpretations shall be published.

## CHAPTER VII
## INFORMATION, ANALYSIS AND TECHNOLOGY

**Article 98 — Purpose limitation**

1. Intelligence information shall be collected, used, matched and disclosed only for a recorded statutory purpose.
2. A new materially different use requires fresh legal, necessity and proportionality assessment and any required warrant.
3. Information shall not be repurposed for taxation, conscription, ordinary employment, political vetting or commercial advantage.
4. System design shall prevent unauthorized browsing and secondary use.

**Article 99 — Data minimization**

1. The Service shall collect and retain only information relevant and reasonably necessary for the authorized purpose.
2. Incidental, excessive, duplicate and clearly irrelevant personal information shall be deleted or irreversibly anonymized promptly.
3. Access shall be restricted by role, case and need, with searchable audit logs.
4. Minimization shall occur at collection, ingest, analysis, dissemination, review and closure.

**Article 100 — Accuracy and reliability**

1. Information shall be marked by source, date, reliability, corroboration, dispute and known limitation.
2. Allegation, inference, automated output and verified fact shall not be presented as equivalent.
3. Material adverse information shall receive reasonable corroboration before operational or policy use.
4. A correction shall be propagated to every known recipient and linked permanently to the original record.

**Article 101 — Retention and deletion**

1. Each information category shall have a published or oversight-approved retention period based on purpose, sensitivity and continuing value.
2. Threat files shall be reviewed periodically and closed when grounds cease; political and unrelated information shall be deleted.
3. A litigation hold, historical archive or oversight preservation shall be segregated from operational use.
4. Deletion shall include copies, indexes, models and downstream systems to the extent technically and legally possible.

**Article 102 — Access and correction rights**

1. A person may request access to and correction of personal intelligence information under data-protection and information law.
2. A refusal shall identify the lawful exemption and be reviewable by the Inspector-General, data-protection authority and court.
3. Neither confirmation nor denial may be used only where acknowledgment itself creates a specific serious harm.
4. The reviewing body shall examine the information fully even where it cannot disclose it to the person.

**Article 103 — Intelligence databases**

1. Every database shall have an approved owner, lawful purpose, data schema, sources, access rules, retention, security and oversight plan.

2. Secret parallel copies, undocumented fields and unrestricted name searches are prohibited.
3. Creation or material expansion of a high-risk database requires impact assessment and Inspector-General review.
4. The data-protection authority may inspect systems under secure arrangements and recommend corrective action.

**Article 104 — Watchlists**

1. A watchlist requires clear statutory purpose, individualized threshold, documented nomination, quality review, expiry and redress.
2. Consequences, recipients, false-positive risk and special rules for children and common names shall be defined.
3. No secret list may itself authorize arrest, passport denial, employment exclusion or property restriction.
4. Every entry shall be periodically revalidated and removed promptly when criteria are not met.

**Article 105 — Artificial intelligence**

1. Artificial intelligence may assist translation, triage, cyber defence, pattern analysis and forecasting but shall remain under accountable human judgment.
2. A high-risk system requires legal authority, impact assessment, validated data, independent testing, explainability, security and ongoing error monitoring.
3. No person shall be targeted, watchlisted or subjected to coercive consequence solely by automated output.
4. Use of a foreign or proprietary model shall not prevent audit, correction, deletion or protection of Eritrean data.

**Article 106 — Predictive analysis**

1. Prediction shall state uncertainty, assumptions, base rates, alternative explanations and risk of feedback loops.
2. A demographic, religious, political or regional proxy shall not substitute for evidence of threatening conduct.
3. Past repression, arrest or intelligence labeling shall not be treated automatically as reliable training data.
4. Operational action requires current individualized grounds independent of a generalized score.

**Article 107 — Cyber intelligence and defence**

1. The Service may identify and analyze hostile cyber threats to constitutional institutions and critical infrastructure.
2. Defensive assistance shall be consensual or legally authorized and shall preserve the mandate of communications, police and defence institutions.

3. Access to private systems, active intrusion and cross-border operation require the authority and warrant applicable to the method.
4. The Service shall not suppress lawful online speech or disrupt a network merely because it carries criticism.

**Article 108 — Information security**

1. The Service shall apply layered physical, personnel, cryptographic, network, supplier and operational security controls.
2. Privileged access shall be minimal, time-limited, separately approved and continuously logged.
3. Independent penetration testing, backup, recovery and insider-risk safeguards shall be maintained.
4. Security measures shall protect oversight access and shall not create unreviewable administrator power.

**Article 109 — Security incidents**

1. Loss, unauthorized access, manipulation, exfiltration or destruction of intelligence information is a security incident.
2. A serious incident shall be contained, preserved, investigated and reported immediately to the Director-General and Inspector-General.
3. The data-protection authority and affected persons shall be notified where law requires and risk permits.
4. Lessons, vendor responsibility, discipline and system correction shall be documented.

**Article 110 — Analytic integrity**

1. An analyst shall be free to state a good-faith assessment and dissent without career retaliation.
2. A manager may edit for evidence, method and clarity but shall not change a conclusion to satisfy policy preference.
3. Significant dissent shall accompany the final assessment or be preserved and identified.
4. The Inspector-General may review allegations of politicization, cherry-picking or suppression.

**Article 111 — Dissemination**

1. A dissemination shall identify recipient, purpose, classification, handling, source reliability, limitations and permitted further use.
2. Personal information shall be included only where necessary for the recipient's lawful function.
3. A recipient shall not further distribute or use intelligence outside authority and shall maintain access logs.
4. Oral briefings affecting a material decision shall be memorialized promptly.

## CHAPTER VIII
## COOPERATION AND EXTERNAL RELATIONS

**Article 112 — Domestic intelligence cooperation**

1. An intelligence-sharing arrangement with an Eritrean public body shall be written, authorized, purpose-specific and subject to audit.
2. It shall define data, threshold, use, onward disclosure, retention, correction, security, incident and termination.
3. A recipient shall possess independent statutory authority to receive and use the information.
4. The Inspector-General shall have access to the arrangement and resulting exchanges.

**Article 113 — Police referrals**

1. A referral to police shall identify information, reliability, collection authority, handling restrictions and known exculpatory matter.
2. Police shall obtain their own judicial authority for arrest, search, evidence acquisition and prosecution.
3. The Service shall not conceal unlawful intelligence collection through parallel reconstruction of an investigative trail.
4. Use in proceedings is governed by fair-trial, disclosure and evidence law.

**Article 114 — Defence cooperation**

1. The Service and defence intelligence may exchange external-threat information and coordinate strategic assessment under written procedures.
2. Defence collection within Eritrea against civilians requires the authority applicable under this Act and the Defence Forces Act.
3. Joint operations shall identify civilian and military command, target, methods, force limits, records and oversight.
4. Military classification shall not prevent Inspector-General, judicial, legislative or audit access.

**Article 115 — Foreign liaison**

1. The Service may cooperate with a foreign intelligence or security body only where cooperation serves a statutory purpose and the partner receives a documented risk assessment.
2. The assessment shall consider legality, human rights, reliability, data protection, torture, political abuse, onward transfer and oversight.
3. High-risk cooperation requires ministerial approval and notice to the Inspector-General.
4. A partner's usefulness shall not excuse complicity in grave abuse.

**Article 116 — Foreign information requests**

1. A foreign request shall identify requesting authority, purpose, target, legal basis, intended use and onward disclosure.
2. The Service shall not perform for a foreign body collection that would be unlawful if undertaken for Eritrea.
3. A request affecting an Eritrean person, protected function or domestic system requires the same warrant safeguards as an Eritrean operation.
4. Approval, refusal, conditions and information supplied shall be recorded.

**Article 117 — Information received from abroad**

1. Foreign information shall be assessed for provenance, legality, reliability, caveats, manipulation and risk of abuse.
2. Information obtained through torture, arbitrary detention, unlawful hacking or political persecution shall be quarantined and reported.
3. It shall not be used to evade domestic collection safeguards or to create an unchallengeable adverse record.
4. Material uncertainty and foreign restrictions shall accompany dissemination.

**Article 118 — Onward disclosure**

1. Eritrean intelligence shall not be disclosed abroad without purpose, necessity, recipient authority, safeguards and a no-unauthorized-onward-transfer condition.
2. Personal information shall be minimized, and anonymous or summary information used where sufficient.
3. Disclosure creating substantial risk of death, torture, persecution, refoulement or arbitrary detention is prohibited.
4. The Service shall monitor material use and suspend cooperation upon breach.

**Article 119 — International arrangements**

1. A material continuing intelligence arrangement shall be written and processed under the Treaty-Making Act where it creates international obligation.
2. An arrangement shall state purpose, authorities, rights safeguards, information rules, finance, dispute, suspension and termination.
3. A secret arrangement shall not authorize domestic power, foreign base, detention, armed operation or unappropriated expenditure.
4. The National Assembly committee and Inspector-General shall receive the full text.

**Article 120 — Foreign personnel in Eritrea**

1. Foreign intelligence personnel may act in Eritrea only under written authorization defining identity, location, activity, duration and Eritrean supervision.
2. They possess no arrest, search, detention, weapons, interception or immunity power except as provided by an Assembly Act or lawfully ratified treaty.

3. Contact with Eritrean residents and access to systems or premises shall comply with this Act.
4. The Inspector-General shall be notified and may inspect activities and records.

**Article 121 — Peaceful regional relations**

1. The Service shall support peaceful relations, early warning and lawful cooperation with neighbouring and regional institutions.
2. It shall not organize proxy forces, political destabilization, cross-border disappearance, assassination or unlawful armed assistance.
3. Diaspora communities shall not be coerced, taxed, threatened or recruited through intelligence authority.
4. A serious foreign threat shall be addressed through constitutional institutions, diplomacy, law enforcement or defence as lawfully appropriate.

## CHAPTER IX
## INSPECTOR-GENERAL OF INTELLIGENCE

**Article 122 — Establishment and independence**

1. An independent Office of the Inspector-General of Intelligence is established as a body corporate.
2. It is independent of the President, Cabinet, Service, Defence Forces, Police Service, prosecutor and political organizations in review and complaint decisions.
3. Its budget shall be a separate appropriation approved by the National Assembly and audited by the Auditor General.
4. No person may direct the Inspector-General to withhold, alter or discontinue a review.

**Article 123 — Appointment**

1. The President shall appoint the Inspector-General from a public merit shortlist prepared by an independent selection panel with approval by two-thirds of the National Assembly.
2. The Inspector-General serves one nonrenewable seven-year term and shall be a person of exceptional integrity and legal, judicial, audit, investigative or intelligence-review competence.
3. A person employed by an intelligence service within the preceding five years is ineligible.
4. Appointment, qualifications, interests and selection report shall be published.

**Article 124 — Removal**

1. The Inspector-General may be removed only for incapacity, serious misconduct, corruption or persistent neglect established by an independent tribunal.
2. The tribunal shall provide notice, evidence, hearing and public reasons subject to narrow security protection.
3. Removal requires approval by two-thirds of the National Assembly.

4. Temporary suspension shall not block urgent oversight and an acting Inspector-General shall be appointed through a pre-established independent procedure.

**Article 125 — Mandate**

1. The Inspector-General shall review legality, necessity, proportionality, reasonableness and efficacy of every intelligence activity.
2. The mandate covers the Service, defence intelligence, police intelligence and any public body or contractor performing national-security intelligence.
3. It includes warrants, sources, operations, data, technology, cooperation, classification, personnel, procurement, finance and ministerial direction.
4. The Inspector-General shall investigate complaints, serious incidents, whistleblower disclosures and matters referred by a court or Assembly committee.

**Article 126 — Unrestricted access**

1. The Inspector-General is entitled to timely access to every place, person, system, record, warrant, source file, legal advice, contract and financial account relevant to the mandate.
2. No classification, executive privilege, foreign caveat, operational sensitivity or agency claim may be asserted against access.
3. Legal professional privilege of a private person remains protected and may be managed through an independent procedure.
4. The head of each institution is personally responsible for complete and timely cooperation.

**Article 127 — Powers**

1. The Inspector-General may summon testimony, require records, enter intelligence premises, inspect systems, conduct tests and preserve evidence.
2. A private dwelling or non-intelligence premises requires consent or judicial warrant.
3. The Inspector-General may engage cleared independent experts and counsel under strict confidentiality.
4. Obstruction, deception, destruction and retaliation shall be referred for disciplinary or criminal action.

**Article 128 — Own-motion and systemic review**

1. The Inspector-General may begin review on own initiative based on risk, random selection, complaint, incident, public report or emerging technology.
2. Every category of intrusive power and every intelligence institution shall receive periodic inspection.
3. A systemic review shall assess not only technical compliance but necessity, outcomes, error, bias, duplication and public cost.
4. The work programme shall remain independent and shall not be limited to matters selected by the executive.

**Article 129 — Immediate protective direction**

1. Where continued activity appears clearly unlawful and creates serious imminent harm, the Inspector-General may direct temporary cessation, segregation or preservation.
2. The direction shall state grounds, scope and duration and shall be served on the responsible head and minister.
3. The institution may seek urgent confidential judicial review but shall comply pending decision.
4. A final remedial order shall follow investigation, response and reasons or court determination.

**Article 130 — Findings and recommendations**

1. A report shall state facts, law, findings, institutional response, corrective action and unresolved disagreement.
2. The Inspector-General may recommend cessation, deletion, notice, discipline, compensation, policy change, training, prosecution referral or legislative amendment.
3. A responsible institution shall respond within sixty days with acceptance, implementation or detailed reasons for refusal.
4. Unresolved illegality shall be referred to the court, prosecutor or National Assembly as jurisdiction requires.

**Article 131 — Reporting**

1. The Inspector-General shall submit classified reports to the responsible minister and National Assembly intelligence committee.
2. An annual public report shall describe activities, access problems, legality, warrants, complaints, incidents, technology, cooperation and implementation without avoidable secrecy.
3. The Service may propose redaction for a specific harm, but the Inspector-General decides subject to expedited judicial review.
4. A public report shall not identify a protected source, active operation or uninvolved person.

**Article 132 — Resources and staff**

1. The Inspector-General shall appoint independent legal, investigative, technical, audit, data and human-rights staff through merit process.
2. Staff shall receive the highest required clearance without Service control over hiring or continued access.
3. A clearance denial affecting oversight staff shall be decided by a warrants judge on confidential evidence.
4. Compensation and facilities shall be sufficient to recruit expertise comparable to the institutions reviewed.

**Article 133 — Coordination with other oversight bodies**

1. The Inspector-General may coordinate with the Auditor General, data-protection authority, police commission, ombud, courts and parliamentary bodies.
2. Coordination shall avoid gaps and duplication while preserving each mandate and complainant rights.
3. Information may be shared securely where necessary and legally permitted.
4. A referral shall be tracked and shall not be used to avoid responsibility.

CHAPTER X
LEGISLATIVE, JUDICIAL AND FINANCIAL OVERSIGHT

**Article 134 — National Assembly Intelligence Committee**

1. The National Assembly shall establish an Intelligence and Security Committee of seven members elected by secret ballot.
2. Members shall reflect gender, regional and viewpoint diversity and shall not include a minister, serving security officer or person with a material Service contract.
3. The Committee shall oversee mandate, policy, administration, expenditure, legality, performance and implementation of Inspector-General findings.
4. It shall not direct an operation, select a target, recruit a source or receive information for political use.

**Article 135 — Committee access**

1. The Committee is entitled to timely access to classified policy, priorities, budgets, audits, significant operations, incidents, agreements and oversight reports.
2. Specific source identity or ongoing tactical detail may be provided through secure limited procedure where broader disclosure creates concrete serious risk.
3. The responsible minister shall state any proposed restriction in writing for review by the Inspector-General and, if disputed, the Supreme Court.
4. No restriction may conceal illegality, expenditure, institutional responsibility or material deception.

**Article 136 — Committee procedure and reporting**

1. The Committee shall adopt secure rules, receive independent staff and may summon officials and request Inspector-General review.
2. Members shall protect lawful secrets but may report illegality through authorized Assembly and judicial channels.
3. It shall issue classified findings and an annual public report with the maximum information consistent with specific security protection.
4. Political use, unauthorized disclosure and false classification shall be addressed through fair Assembly discipline and law.

**Article 137 — Judicial oversight beyond warrants**

1. Courts retain jurisdiction to review intelligence legality, warrants, rights limitations, detention allegations, evidence and remedies.
2. A court may inspect all relevant classified information, appoint security-cleared counsel and hold a closed portion only where strictly necessary.
3. A public judgment shall state legal principles and result with narrow redaction.
4. Neither state-secrets assertion nor foreign caveat shall extinguish jurisdiction or an effective remedy.

**Article 138 — Auditor General**

1. The Auditor General shall audit every intelligence appropriation, account, asset, procurement, covert payment, foreign assistance and contingent liability.
2. Audit access is complete and shall not depend on permission from the Service or executive.
3. Operational detail may be reported securely, but aggregate expenditure, qualification and material control failure shall be reported publicly.
4. An unauditable fund, cash pool, business or foreign account is prohibited.

**Article 139 — Advocate General and prosecution**

1. The Advocate General may advise the Government on intelligence legality without controlling independent courts, prosecutors or the Inspector-General.
2. Evidence of an offence shall be referred to the independent prosecutor according to law.
3. The Service shall not condition, delay or withdraw referral to protect reputation or political interest.
4. Prosecutorial decision shall not be directed by intelligence officials or classification alone.

**Article 140 — Public Finance Management Act**

1. All Service money is public money governed by appropriation, control, accounting and reporting under the Public Finance Management Act.
2. A classified programme may use protected schedules but remains within the approved total and control framework.
3. Virement, emergency expenditure and write-off require the same lawful authority applicable elsewhere in government.
4. Secrecy shall not prevent traceable responsibility for every payment.

**Article 141 — Public Procurement Act**

1. Intelligence procurement is governed by the Public Procurement Act, including any narrowly tailored security procedure authorized there.
2. Direct or classified procurement requires recorded necessity, competition to the maximum practicable extent, price testing, conflicts and audit.

3. A front company, nominee or foreign intermediary shall not conceal beneficial ownership from procurement and oversight institutions.
4. Surveillance technology requires human-rights, cyber-security, interoperability, maintenance and vendor-control assessment.

**Article 142 — Foreign assistance**

1. Money, equipment, training, data access or personnel support from a foreign source shall be recorded and accepted only under lawful authority.
2. Terms, ownership, recurring cost, data access, operational influence and human-rights risk shall be assessed before acceptance.
3. Foreign assistance shall not create an off-budget capability, exclusive allegiance or hidden obligation.
4. The Auditor General, Inspector-General and Assembly committee shall receive complete information.

**Article 143 — Oversight security**

1. Oversight institutions shall maintain secure facilities, vetted staff, handling rules and incident response proportionate to information received.
2. Security requirements shall be administered independently and shall not permit the Service to control findings or staffing.
3. Unauthorized disclosure shall be investigated fairly without presuming that criticism or disagreement proves disclosure.
4. Security shall facilitate rather than defeat democratic oversight.

## CHAPTER XI
## COMPLAINTS, DISCLOSURES AND REMEDIES

**Article 144 — Right to complain**

1. Any person may complain to the Inspector-General about intelligence action, information, adverse consequence, retaliation or failure to act.
2. A complaint may be filed securely, orally, electronically, through counsel or by a representative.
3. No fee, citizenship, residence, standing or proof of surveillance is required to initiate reasonable inquiry.
4. The Service shall publish accessible complaint information without collecting complainants for intelligence purposes.

**Article 145 — Complaint investigation**

1. The Inspector-General shall acknowledge, assess jurisdiction, preserve evidence and investigate fairly and promptly.
2. The complainant shall receive opportunity to provide information and a result with reasons to the greatest lawful extent.

3. Neither confirmation nor denial may protect a specific operation, but the Inspector-General shall still determine legality and remedy.
4. A manifestly unfounded or abusive complaint may be closed with reasons and review information.

**Article 146 — Protected disclosures**

1. A current or former officer may disclose suspected illegality, abuse, deception, danger, corruption or gross waste to the Inspector-General, Auditor General, prosecutor, court or Assembly committee.
2. The person may bypass command where command is implicated, unsafe or unresponsive.
3. Disclosure made through an authorized channel does not breach secrecy and shall not attract retaliation.
4. Where all authorized channels fail and grave imminent harm persists, public-interest disclosure is governed by whistleblower law and judicial protection.

**Article 147 — Protection against retaliation**

1. Dismissal, transfer, clearance loss, threat, prosecution, surveillance, blacklisting, benefit loss or harm to family in retaliation is prohibited.
2. The Inspector-General or court may order interim protection, reinstatement, transfer, confidentiality, compensation and discipline.
3. The employer bears the burden to show that a materially adverse action following protected disclosure was unrelated where the circumstances raise a reasonable inference of retaliation.
4. Knowingly false malicious disclosure may be addressed through fair process without discouraging good-faith error.

**Article 148 — Available remedies**

1. A court may declare illegality, stop activity, quash a warrant, order deletion or correction, notify a person, return property and award compensation.
2. It may exclude or restrict unlawfully obtained information, require policy change, training, audit or independent investigation.
3. A remedy shall address continuing digital copies, recipients, watchlists, models and consequences.
4. Official immunity does not protect bad faith, knowing illegality, torture, disappearance, corruption or destruction of evidence.

**Article 149 — No secret evidence as sole basis**

1. A person shall not lose liberty, nationality, passport, employment, licence, property or public benefit solely on intelligence that the person cannot effectively challenge.
2. A court may use protected procedures, summaries, admissions, independent counsel or other means to preserve both security and fair process.
3. If sufficient fairness cannot be achieved, the adverse consequence shall not be imposed.

4. Intelligence is not proof of crime and shall be tested according to applicable evidence standards.

**Article 150 — Limitation periods**

1. A claim concerning covert intelligence accrues when the person knew or reasonably could have known sufficient facts to seek remedy.
2. Secret concealment and unlawful failure to notify suspend limitation to the extent provided by procedural law.
3. A grave violation including torture or disappearance shall not be protected by an unreasonably short limitation period.
4. Preservation duties continue while a complaint, review or proceeding is reasonably anticipated.

**Article 151 — Public-interest standing**

1. A qualified human-rights, professional or public-interest body may challenge a systemic intelligence rule or practice where affected persons cannot reasonably do so.
2. The court shall ensure concrete issues, responsible representation and protection of individuals.
3. Standing does not authorize access to operational information beyond what fair adjudication requires.
4. Systemic remedy may accompany individual relief.

CHAPTER XII
FINANCE, RECORDS AND CLASSIFICATION

**Article 152 — Annual budget**

1. The Service shall prepare a complete annual budget including personnel, operations, technology, property, procurement, foreign assistance and contingent obligations.
2. The responsible minister shall submit it through the constitutional budget process without an undisclosed supplement.
3. The Assembly committee shall receive detailed classified schedules and fiscal-risk explanation.
4. Appropriation shall not identify a source or active operation publicly where specific harm would result.

**Article 153 — Covert expenditure**

1. A covert payment requires authorized purpose, approving officer, recipient control, amount, date and protected supporting record.
2. Cash use shall be exceptional, limited, reconciled and independently reviewed.
3. Source safety may justify protected identity but not absence of accountable verification.
4. Personal, political, punitive and unlawful payments are prohibited and recoverable.

**Article 154 — Assets and premises**

1. Every Service land interest, building, vehicle, weapon, device, account and material asset shall be registered in a secure auditable inventory.
2. A covert asset may use protected description but shall have verified existence, custodian, value and authority.
3. No unregistered prison, interrogation room, commercial estate or foreign facility may be maintained.
4. Disposal shall follow public-property and procurement law with secure data destruction.

**Article 155 — Operational records**

1. The Service shall create contemporaneous records of tasking, approval, collection, analysis, dissemination, incident, expenditure and closure.
2. Oral direction affecting rights, money or operation shall be memorialized promptly.
3. Records shall be protected from unauthorized change through immutable logs and version control.
4. Failure to create a required record is itself a compliance breach and shall not benefit the institution.

**Article 156 — Preservation and archives**

1. Records shall be retained under an approved schedule balancing accountability, operational need, privacy and historical value.
2. Records concerning detention, disappearance, torture, political surveillance, deaths, major expenditure and transitional conduct shall not be destroyed.
3. The National Archives shall receive historically valuable records after security review and retain professional custody.
4. Operational restrictions shall be reviewed periodically and shall not prevent eventual public history where harm has ended.

**Article 157 — Classification authority**

1. Information may be classified only where unauthorized disclosure would create a specific identifiable harm to lawful national security.
2. Classification levels, authorities, markings, duration and review shall be prescribed by an Assembly Act or regulations strictly under this Act.
3. Information shall not be classified to conceal illegality, abuse, corruption, error, embarrassment, inefficiency or political advantage.
4. The classifier bears responsibility for reasons and review date.

**Article 158 — Declassification**

1. Classification expires on the stated date unless renewed on current specific grounds.
2. Systematic review shall prioritize constitutional history, completed operations, public controversy and records older than ten years.

3. Partial disclosure and redaction shall be preferred to total withholding.
4. The Inspector-General, information commission and court may review and order declassification within their mandates.

**Article 159 — Duty of secrecy**

1. Personnel and authorized recipients shall protect lawfully classified information and personal intelligence data.
2. Secrecy is limited to information genuinely requiring protection and does not prohibit authorized oversight, court process or protected disclosure.
3. A prosecution for disclosure requires proof of knowing unauthorized disclosure and actual or probable serious harm, subject to public-interest safeguards in law.
4. Administrative classification alone does not create a criminal offence.

**Article 160 — Records of deceased and missing persons**

1. The Service shall assist lawful efforts to determine the fate of missing, detained or deceased persons and shall preserve relevant records.
2. Families and truth-seeking institutions shall receive information to the greatest extent compatible with a specific current risk and fair process.
3. No officer may invoke secrecy to conceal a burial, death, disappearance or place of detention.
4. A dispute over disclosure shall receive expedited independent review.

**Article 161 — Annual public information**

1. The Service shall publish mandate, organization, legal instruments, senior leadership, budget aggregate, priorities summary, statistics and contact information.
2. Statistics shall include warrants, emergencies, datasets, errors, complaints, discipline, foreign arrangements and records review in nonidentifying form.
3. Public reports shall describe improvements, failures and unresolved oversight recommendations.
4. A general claim of national security shall not justify omission of all meaningful information.

## CHAPTER XIII
## TRANSITIONAL, REPEAL AND FINAL PROVISIONS

**Article 162 — Immediate preservation order**

1. Upon publication, every public body shall preserve intelligence, security, detention, surveillance, source, personnel, financial and operational records.
2. Deletion, alteration, concealment, transfer abroad and unauthorized removal are prohibited.
3. The Inspector-General-designate, Auditor General and courts may issue protective directions before full institutional commencement.

4. Ordinary automatic-deletion schedules are suspended for twelve months pending lawful review.

**Article 163 — Inventory of institutions and capabilities**

1. Within ninety days, the Government shall identify every intelligence unit, premises, database, account, weapon, interception system, company, agreement and foreign relationship.
2. The inventory shall distinguish legal authority, custodian, current use, risk and proposed disposition.
3. A hidden or unclaimed capability shall be secured immediately and reported to oversight institutions.
4. A public summary shall describe the process and categories without exposing protected persons.

**Article 164 — Audit of detention and coercive activity**

1. Every place previously used by an intelligence or security body for custody, interrogation or coercive questioning shall be identified and inspected.
2. Any person found in custody shall be brought before a court immediately or released.
3. Missing-person, death, torture and disappearance evidence shall be secured and referred for independent investigation.
4. No premises shall be transferred, renovated or destroyed until inspection and evidence preservation are complete.

**Article 165 — Review of personnel**

1. Existing personnel shall undergo independent status, qualification, integrity and conduct review before permanent appointment to the Service.
2. Review shall distinguish individual responsibility from institutional membership and shall reject collective guilt or automatic immunity.
3. Notice, evidence, response, representation and review shall be provided consistent with necessary source protection.
4. A person not appointed retains lawful employment, pension and due-process rights subject to proven misconduct.

**Article 166 — Dissolution of unauthorized bodies**

1. An intelligence, security, political-monitoring or detention body lacking authority under an Assembly Act shall cease operation on commencement.
2. Its personnel, property, funds and records shall be secured under a published transitional direction and independent oversight.
3. No body shall be preserved merely by transfer to the Presidency, military, party, ministry, public enterprise or private company.
4. Necessary lawful functions may recommence only through the institutions and procedures in this Act.

**Article 167 — Legacy files and watchlists**

1. Political, religious, diaspora, journalist, union, student, village and other legacy files shall be reviewed for lawful continuing purpose.
2. A record unsupported by current statutory threat grounds shall be removed from operational systems and preserved only where required for accountability or history.
3. Every watchlist and adverse intelligence consequence shall be suspended until criteria, accuracy and authority are independently verified.
4. Affected persons shall receive correction and notice when lawful risk permits.

**Article 168 — Legacy commercial and foreign arrangements**

1. The Government, Auditor General and Inspector-General shall inventory Service businesses, assets, foreign accounts, gifts, equipment and cooperation agreements.
2. Commercial interests shall be transferred to lawful public ownership administration, privatized or liquidated under applicable Assembly Acts.
3. Foreign arrangements inconsistent with this Act shall be suspended, renegotiated or terminated through lawful process.
4. Continuity does not validate corruption, unauthorized debt, rights abuse or secret sovereignty transfer.

**Article 169 — Transitional appointments**

1. The Director-General and Inspector-General shall be appointed within six months after publication through the procedures in this Act.
2. A temporary administrator may preserve life, records, systems and lawful essential warning but shall not commence a new intrusive operation except under judicial warrant.
3. The temporary administrator shall report monthly to the responsible minister, Assembly committee and designated transitional reviewer.
4. Temporary appointment expires upon appointment of the Director-General and in any event after nine months.

**Article 170 — Regulations**

1. The President may issue regulations on recommendation of the responsible minister after consultation with the Inspector-General for administrative implementation of this Act.
2. Regulations may address organization, personnel, secure records, warrant forms, source administration, provider assistance, classification, statistics and transition.
3. They shall not create a threat category, intrusive power, offence, detention authority, bulk-surveillance programme or exception from independent oversight.
4. Draft regulations shall be published for consultation, and a sensitive operational annex shall receive Inspector-General and Assembly committee review.

**Article 171 — Service policies**

1. The Director-General may issue internal policies consistent with this Act and regulations.
2. A policy affecting public rights, complaint access, provider duties or general interpretation shall be published with only necessary operational redaction.
3. No policy may substitute for a warrant or create power, penalty, secrecy offence or expenditure authority.
4. Every policy shall have an owner, approval date, review date, version history and oversight access.

**Article 172 — Review of prior instruments**

1. The Advocate General, Inspector-General and responsible minister shall review prior proclamations, legal notices, directives, orders and practices concerning intelligence within twelve months.
2. They shall authenticate text and identify what is repealed, obsolete, inconsistent, unpublished or requires express saving.
3. A repeal or saving schedule shall be submitted to the National Assembly with reasons and shall not silently alter historical instruments.
4. An unpublished direction conferring surveillance, detention, finance or coercive power is not preserved.

**Article 173 — Periodic independent review**

1. An independent public review of this Act shall begin four years after commencement and at intervals not exceeding five years thereafter.
2. It shall assess threats, efficacy, rights, warrants, technology, data, cooperation, expenditure, complaints, remedies and institutional culture.
3. The review shall receive evidence from oversight bodies, courts, personnel, victims, journalists, lawyers, academia, diaspora and civil society.
4. A public report and Government response shall be submitted to the National Assembly with proposed amendments.

**Article 174 — Commencement**

1. Articles prohibiting detention, torture, disappearance, political surveillance, destruction of records and unauthorized expenditure apply immediately upon publication.
2. The warrant and oversight Chapters commence within six months and no intrusive power may be exercised before they are operational.
3. The remaining provisions commence on a date not later than nine months after publication fixed by a published presidential regulation.
4. Implementation requires lawful appropriation, independent appointments, secure courts and a public transitional plan.

Made at Asmara, this ___ day of __________ 2026.

THE NATIONAL ASSEMBLY OF ERITREA