Confidentiality Provisions

Asylum Research & Global Assistance

Preamble

Asylum Research & Global Assistance operates within a field in which confidentiality is not merely an internal preference but a foundational duty of **legal compliance, ethical responsibility, humanitarian integrity, and operational security**. The Organization routinely handles information of an exceptionally sensitive character, including but not limited to **client identities, personal histories, asylum narratives, legal strategies, supporting evidence, witness statements, donor information, internal assessments, operational logistics, security protocols, partner communications, and other non-public materials** the disclosure of which could cause severe legal, personal, financial, reputational, or physical harm. These Confidentiality Provisions are established to ensure that all such information is protected with the highest degree of care, that disclosure occurs only under strictly controlled and lawful circumstances, and that any misuse is addressed with uncompromising seriousness.

1. Scope and Fundamental Obligation

All individuals, whether staff members, contractors, consultants, volunteers, temporary personnel, advisors, or any other persons granted access to the Organization's information systems, records, communications, or internal processes, shall be bound by an absolute duty to maintain confidentiality. This duty applies to all information obtained in the course of service to, association with, or engagement by Asylum Research & Global Assistance, whether such information is received orally, in writing, electronically, visually, or by any other means, and whether or not it is expressly marked as confidential. The obligation of confidentiality extends to information relating to present, former, and prospective clients, partners, donors, beneficiaries, third parties, and the internal affairs of the Organization. **No person may treat access as a privilege for personal convenience, external advantage, or informal sharing.** Access is granted solely for legitimate organizational purposes and only to the extent strictly necessary for the performance of assigned duties.

2. Classification and Handling of Information

All information under the custody or control of the Organization shall be treated according to its sensitivity, legal significance, and potential harm in the event of unauthorized disclosure. Information relating to client protection, immigration status, humanitarian claims, legal representation, donor records, financial data, internal correspondence, risk assessments, source identities, or security matters shall be regarded as **restricted and highly sensitive information** and subject to the strictest controls. Such information shall be used only for authorized purposes, stored only in approved systems, and accessed only by persons with a demonstrable need to know. No confidential material may be removed, reproduced, transmitted,

summarized, photographed, forwarded, uploaded, published, or otherwise disseminated except in accordance with written authorization or clear legal necessity. **Informal convenience, administrative habit, or assumed permission shall never constitute lawful authority.**

3. Non-Disclosure and Limited Permissible Use

Confidential information shall be used exclusively for the purpose for which it was disclosed or created and shall not be repurposed for personal, political, commercial, academic, media, advocacy, or external organizational use without prior written authorization. A recipient of confidential information shall not disclose such information to any third party unless such disclosure is expressly approved by the Organization and strictly limited to the minimum necessary scope. Where disclosure is required by law, court order, regulatory obligation, or binding governmental demand, the person or unit receiving the request shall, to the maximum extent legally permissible, **notify the Organization immediately**, preserve the confidentiality of all non-disclosable materials, and cooperate in any lawful effort to narrow, challenge, or limit the disclosure. Under no circumstances shall any individual voluntarily expand the scope of disclosure beyond what is expressly required or authorized. **The duty is to protect first, disclose only when compelled, and disclose no more than is legally unavoidable.**

4. Security, Storage, and Protective Measures

Every person with access to confidential information shall maintain strict safeguards designed to prevent unauthorized access, loss, alteration, interception, duplication, or destruction. Such safeguards include, without limitation, the use of secure passwords, multifactor authentication where available, encrypted storage and transmission, locked physical storage, clean-desk discipline, controlled printing, secure disposal, and the avoidance of unapproved applications, devices, or communication channels. Confidential information shall not be stored on personal devices, unsecured cloud services, private email accounts, removable media, or any platform not expressly approved by the Organization. Conversations involving sensitive matters shall be conducted only in private settings and only with persons authorized to participate. Documents shall not be left unattended, displayed in public view, or discussed within earshot of unauthorized persons. **Every individual shall act as a custodian of trust, not as a casual holder of data.** The standard of care required is not ordinary caution but heightened professional vigilance commensurate with the risks inherent in asylum-related and humanitarian work.

5. Breach, Reporting, and Consequences

Any actual, suspected, or potential breach of confidentiality shall be reported immediately to the appropriate designated authority within the Organization. Delay, concealment, minimization, or informal correction shall be treated as aggravating conduct. Upon notice of a breach, the Organization may implement containment measures, restrict access, conduct an internal review, notify affected persons where appropriate, preserve evidence, and take any further action necessary to mitigate harm and comply with legal obligations. Any unauthorized disclosure, negligent handling, intentional misuse, or reckless disregard of confidentiality obligations shall constitute a serious violation of professional duty and organizational trust. Depending on the gravity of the conduct, consequences may include **immediate removal from access, suspension, termination of engagement, revocation of privileges, referral to licensing**

or regulatory bodies, civil action, and, where applicable, criminal referral. The Organization shall exercise zero tolerance toward deliberate breaches and will treat any compromise of protected information as a matter of profound institutional consequence.

6. Return, Retention, and Survival of Obligations

Upon request, upon conclusion of an assignment, or upon termination of any relationship with the Organization, all confidential materials, copies, extracts, summaries, recordings, and derivative works shall be returned, securely deleted, or otherwise disposed of in accordance with the Organization's instructions. No person shall retain confidential information after their authorization has ended, whether in physical, electronic, or reconstructed form. The duty of confidentiality shall survive termination of employment, contract, volunteer service, or any other association with the Organization and shall continue for so long as the information remains confidential or protected by law. **The end of service does not extinguish the duty of loyalty, discretion, or protection.**

7. Ethical Standard and Institutional Expectation

These Confidentiality Provisions are not limited to minimum legal compliance. They reflect the Organization's higher standard of **ethical responsibility, disciplined discretion, and uncompromising protection of vulnerable persons and sensitive institutional interests**. Every person entrusted with access to confidential information is expected to understand that confidentiality is integral to the credibility, safety, and legitimacy of Asylum Research & Global Assistance. Breach of confidence is not a technical misstep; it is a serious failure of judgment, trust, and professional integrity. The Organization therefore requires not only compliance with the letter of these provisions, but faithful adherence to their spirit: **protect the vulnerable, preserve the integrity of the work, and disclose nothing except what is strictly necessary and lawfully permitted.**

I. INFORMATION CLASSIFICATION

ASYLUM RESEARCH & GLOBAL ASSISTANCE maintains an uncompromising information governance standard grounded in **confidentiality, necessity, proportionality, and strict internal accountability**. Every item of information handled by the organization shall be classified according to its sensitivity, the foreseeable harm that may arise from unauthorized disclosure, the legal and ethical obligations attached to it, and the operational consequences of misuse, alteration, or loss. Classification is not a formality; it is a **binding control mechanism** intended to protect clients, beneficiaries, staff, institutional integrity, legal privilege, security interests, and the organization's broader humanitarian and investigative mission. Any ambiguity in classification must be resolved **in favor of greater protection**, not convenience.

A. Highly Confidential

Highly Confidential information constitutes the most restricted class of information held by the organization and includes any material whose unauthorized disclosure, access, transmission, duplication, or discussion could cause **serious legal, physical, psychological, reputational, operational, or strategic harm**. This category includes, without limitation, **client identities**

and personal details such as names, residential or mailing addresses, telephone numbers, email addresses, identifying documents, family relationships, immigration-related data, and any other information capable of directly or indirectly identifying an individual. It also includes **legal case strategies, litigation planning, evidentiary assessments, witness preparation materials, privileged communications, and any evidence not yet disclosed to an opposing party** or otherwise subject to legal privilege, protective order, or confidentiality obligation. In addition, **medical records, psychological evaluations, trauma-related disclosures, vulnerability assessments, and any sensitive health-related data** fall within this class, given the profound duty of care and the potential for irreversible harm if exposed. Likewise, **security-related information** concerning personnel, field operations, safe houses, facility access systems, movement protocols, emergency procedures, protective measures, or physical and digital safeguarding arrangements is deemed Highly Confidential because its disclosure may create direct threats to life, liberty, and organizational continuity.

Handling of Highly Confidential information shall be governed by the **strictest internal controls**. Access is granted strictly on a **need-to-know basis** and only to personnel expressly authorized by role, mandate, and documented responsibility. Such information shall not be accessed casually, discussed informally, forwarded indiscriminately, or stored in unsecured environments. It must be maintained in **encrypted storage**, transmitted only through approved secure channels, and protected by layered technical and administrative safeguards appropriate to the sensitivity of the material. Printed copies, if absolutely necessary, must be controlled, logged, and physically protected against unauthorized viewing or removal. Any sharing outside the authorized circle, whether intentional or negligent, is a material breach of duty and may trigger disciplinary, contractual, legal, and operational consequences. **The preservation of confidentiality in this category is absolute in principle and exceptional only where compelled by lawful authority or expressly sanctioned by senior authorization and applicable law.**

B. Confidential

Confidential information is information that, while not necessarily rising to the level of immediate existential risk associated with Highly Confidential material, still requires **meaningful restriction, deliberate handling, and controlled internal circulation**. This category includes **donor agreements, grant terms, funding conditions, financial commitments not yet public, negotiated obligations, draft partnership arrangements, and any non-public commercial or institutional commitments** that could affect bargaining position, donor confidence, contractual leverage, or institutional reputation if prematurely disclosed. It also includes **board minutes, committee records, internal strategic discussions, decision-making materials, policy deliberations, and sensitive management communications**, particularly where those materials reflect unfinished positions, internal disagreements, investigative direction, or governance planning. Additionally, **performance data not yet published**, including operational metrics, impact assessments, internal reviews, compliance findings, audit materials, and program evaluations, shall be treated as Confidential until officially released or otherwise designated for broader dissemination.

Handling of Confidential information requires **limited distribution within the organization** and the consistent application of standard protective measures. Such information shall be clearly marked **"Confidential"**, stored in secured systems or controlled repositories, and shared only with personnel whose duties genuinely require access. The organization must preserve the integrity of this information through appropriate document control, version management, and retention practices, including the application of a **defined retention period** consistent with legal, regulatory, contractual, and operational requirements. Confidential information shall not be disclosed externally without authorization, nor used for purposes unrelated to the reason for its collection or creation. Internal recipients remain responsible for ensuring that disclosure is **purpose-limited, documented where necessary, and never broader than operational necessity requires**. The standard governing this class is one of disciplined restraint: confidentiality is not presumed to be optional, and convenience is never a lawful justification for disclosure.

C. Internal

Internal information consists of non-public organizational material intended for use within ASYLUM RESEARCH & GLOBAL ASSISTANCE and not designated for external release. This category includes **policy documents, procedures, internal guidance, routine administrative communications, training materials, organizational charts, staffing decisions not yet announced, internal schedules, and operational notices**. While this information may not contain the same level of inherent sensitivity as Confidential or Highly Confidential materials, it remains proprietary and functionally important to the organization's orderly governance, institutional coherence, and operational efficiency. Unauthorized external release may still cause confusion, undermine internal alignment, disrupt workforce planning, or expose the organization to avoidable misinterpretation and reputational harm.

Handling of Internal information shall be limited to **staff access only**, subject to standard protective measures and ordinary workplace security controls. This includes responsible storage, controlled distribution, and the avoidance of unnecessary duplication or external forwarding. Internal information should be treated with professional discretion, because even ordinary operational content may become sensitive when detached from context, circulated out of sequence, or interpreted by persons without proper authorization. Staff members must exercise **sound judgment, restraint, and procedural discipline** in relation to all internal materials. The fact that information is not classified as Confidential does not reduce the expectation that it be handled responsibly; rather, it confirms that access is granted for organizational use only and not for personal convenience, informal sharing, or public exposure.

In all cases, classification shall be determined by the highest reasonably applicable level of sensitivity, not by the lowest convenient reading. Information must be protected in a manner proportionate to the harm that may result from misuse, and all personnel are under a continuous obligation to respect classification labels, confidentiality boundaries, and lawful handling requirements. **No person is entitled to access information merely because they can. Access exists only where it is authorized, necessary, and consistent with the organization's ethical and legal obligations.**

II. OWNERSHIP & USE RIGHTS

All information, materials, data, findings, analyses, notes, drafts, compilations, memoranda, correspondence, case summaries, investigative outputs, internal communications, and any other content received, created, assembled, processed, interpreted, or otherwise generated by ARGA personnel in the course of their duties shall be deemed the exclusive organizational property of ASYLUM RESEARCH & GLOBAL ASSISTANCE ("ARGA"), to the fullest extent permitted by applicable law. This principle applies regardless of the format, medium, stage of completion, authorship contribution, or location of storage, and extends equally to original records and to any derivative, revised, annotated, translated, summarized, or reformatted version thereof. No personnel member acquires any personal ownership interest, implied license, proprietary entitlement, or independent right of control by virtue of creation, access, possession, or use.

All intellectual property produced in the course of ARGA operations shall belong exclusively to ARGA. This includes, without limitation, **reports, research memoranda, legal analyses, case law compilations, policy frameworks, templates, methodologies, work products, reference materials, proprietary assessments, training content, internal guidance, and all compilations or arrangements of information that reflect ARGA's labor, judgment, expertise, coordination, or editorial input**. Where personnel contribute to the development of such materials, their contributions shall be treated as made within the scope of organizational service and for the benefit of ARGA alone. Personnel shall take all reasonable and required steps to secure, preserve, assign, and confirm ARGA's ownership interest in such materials, including executing any documents reasonably necessary to evidence, perfect, or defend ARGA's rights.

No personnel member may exploit, disclose, repurpose, reproduce, adapt, distribute, publish, commercialize, or otherwise use confidential or proprietary information for personal benefit, third-party benefit, or external projects without the express prior written approval of authorized ARGA leadership. This prohibition applies whether the intended use is direct or indirect, immediate or future, compensated or uncompensated, and whether the use occurs during or after the period of engagement. It expressly includes the use of ARGA work product, internal reasoning, operational methods, source materials, client-related information, or non-public observations as a basis for private consulting, independent research, publication, presentation, training, advocacy, or any external endeavor. **Silence, informal permission, custom, prior tolerance, or access alone shall never constitute authorization.** Any permitted use must be narrowly defined, documented in writing, and confined strictly to the scope, duration, and purpose expressly approved.

Client information is held by ARGA in trust and with the highest duty of fidelity, restraint, and purpose limitation. Such information may be accessed, processed, reviewed, stored, transmitted, or otherwise used **only for the specific purpose for which it was lawfully and properly shared with ARGA** and only by personnel whose duties require such access. Client information shall never be treated as a general organizational asset available for unrelated operational, educational, reputational, commercial, or research purposes. ARGA personnel must preserve the confidentiality, integrity, and contextual sensitivity of all client data

and must not disclose, summarize, quote, characterize, or infer client information beyond the minimum necessary for authorized performance. Any ambiguity concerning permissible use shall be resolved in favor of protection, limitation, and non-disclosure.

Any unauthorized retention, copying, extraction, transmission, publication, or reuse of organizational or client information constitutes a serious breach of duty and may result in immediate disciplinary action, revocation of access, legal action, and any other remedy available to ARGA under contract, policy, or applicable law. ARGA shall retain full authority to determine whether any act, omission, or attempted use has exceeded the bounds of authorization, and personnel are expected to exercise uncompromising diligence, restraint, and loyalty in protecting all ARGA-owned and client-confidential materials.

III. AUTHORIZED DISCLOSURES

A. Internal Disclosures

Disclosure of Confidential Information within **ASYLUM RESEARCH & GLOBAL ASSISTANCE** shall be strictly limited to personnel who demonstrably require such information for a legitimate business purpose and whose access is necessary, proportionate, and directly connected to the performance of assigned duties. **No internal disclosure shall be made on the basis of convenience, hierarchy, informal request, or generalized operational interest.** Access shall follow the **need-to-know principle**, and the determination of such need shall rest with the relevant supervisor or designated authority, acting in accordance with internal access protocols, operational necessity, and the principle of least privilege.

All internal access authorizations must be **documented in staff access records**, including the identity of the recipient, the scope of information disclosed, the business justification, the date and time of disclosure, and the approving authority. Internal disclosure does not constitute unrestricted access: personnel receiving information remain bound by confidentiality, duty of care, and the obligation to use the information exclusively for the approved purpose. Any further circulation, copying, extraction, discussion, or storage beyond the approved scope is prohibited unless separately authorized in writing. Where doubt exists as to whether internal disclosure is necessary, the presumption shall favor **non-disclosure until formal review and approval are obtained**.

B. External Disclosures

External disclosure of Confidential Information shall occur only where it is **lawfully required, expressly authorized, narrowly tailored, and strictly controlled**. Under no circumstances may external information be released on an informal basis, by verbal assurance alone, or on the assumption that a requesting party is entitled to receive it. All external disclosures must be evaluated against the principles of legality, necessity, proportionality, confidentiality, and documented accountability.

Where disclosure is sought in connection with **governmental, administrative, investigative, or judicial proceedings**, release shall occur only pursuant to **valid legal process**, including, where applicable, a subpoena, warrant, court order, statutory notice, or other compulsory instrument issued by a competent authority. Prior to disclosure, the request must be reviewed for

authenticity, jurisdictional validity, scope, temporal limits, and legal sufficiency. The organization shall disclose **only the minimum information legally required**, and where the law permits, shall seek clarification, limitation, protective treatment, or confidentiality restrictions to prevent unnecessary dissemination.

Where disclosure is required by **mandatory legal obligation**, including but not limited to child protection, safeguarding, crime prevention, anti-fraud duties, sanctions compliance, or other statutorily mandated reporting obligations, the organization shall comply to the extent required by law and no further. Such disclosure must remain confined to the legally mandated subject matter and recipients. The existence of a legal obligation does not authorize broader sharing, interpretive commentary, or collateral disclosure. The organization shall act with **moral firmness and legal precision**, ensuring that compliance with law never becomes a pretext for avoidable over-disclosure.

Where disclosure is based on **client consent**, such consent must be **prior, written, informed, specific, and verifiable**. The authorization must clearly identify the information to be disclosed, the recipient or category of recipient, the purpose of disclosure, the duration of validity, any territorial or contextual limits, and any express restrictions on onward transfer. Consent shall be construed narrowly, and **no disclosure may exceed the exact scope authorized**. A general or ambiguous authorization shall not be interpreted as permission for broad dissemination. If the request falls outside the written authorization, fresh consent or a separate lawful basis must be obtained before any release occurs.

Where disclosure is made to **donors, auditors, inspectors, or other contractual oversight parties**, only the information expressly required by the governing agreement, audit terms, regulatory framework, or due diligence mandate may be shared. Such disclosure shall be limited to the **minimum necessary information**, and only after confirming that the recipient is bound by confidentiality obligations, data protection commitments, and use restrictions consistent with the organization's standards. Any request for additional material beyond the agreed scope must be escalated for formal review and may be denied where disclosure would compromise privacy, privilege, security, operational integrity, or the legitimate interests of clients and stakeholders.

C. Prohibited Disclosures

The following disclosures are strictly prohibited unless a separate lawful basis and written authorization have been expressly approved: **disclosure to media representatives**, whether direct or indirect, absent explicit authorization and prior vetting by the Communications Director or other designated authority; disclosure to **third-party researchers, contractors, consultants, technology vendors, or service providers** unless a valid data processing agreement, confidentiality undertaking, and security review are in place; disclosure through **social media, online platforms, public forums, informal digital channels, or any other public medium**; and disclosure to **personal networks, relatives, friends, or acquaintances**, regardless of intent, relationship, urgency, or perceived harmlessness.

It is expressly understood that **good faith does not excuse unauthorized disclosure**. Even disclosures made without malicious intent may cause irreversible harm, including legal liability, reputational damage, breach of trust, privacy violations, compromise of vulnerable persons, and

interference with investigations or protective measures. Accordingly, all personnel must treat confidentiality as a core professional duty, not as a matter of discretion. Where an individual is uncertain whether a disclosure is permitted, the individual must **withhold the information and seek formal guidance before any communication occurs**.

Any disclosure not expressly permitted under this Section shall be deemed **unauthorized**. Unauthorized disclosure constitutes a serious breach of professional duty and may result in disciplinary action, civil liability, contractual consequences, regulatory reporting, and referral to law enforcement or other competent authorities where warranted. The organization reserves the right to take all lawful measures necessary to contain harm, preserve evidence, notify affected parties where required, and enforce its rights with full rigor.

IV. RETENTION & DESTRUCTION

ASYLUM RESEARCH & GLOBAL ASSISTANCE maintains a **strict, lawful, and documentable records retention and destruction framework** designed to ensure compliance with applicable legal, regulatory, fiscal, contractual, and operational obligations. All records must be preserved for the full retention period applicable to their category, and no record may be altered, concealed, prematurely discarded, or destroyed in a manner inconsistent with this policy. **Retention periods shall be applied conservatively and in a manner that preserves institutional integrity, evidentiary reliability, and compliance readiness.**

1. Client Files

All **client files**, whether maintained in physical, electronic, or hybrid form, shall be retained for **seven (7) years following closure of the matter, engagement, case, or service relationship**, unless a longer retention period is required by law, regulation, contractual obligation, litigation hold, audit requirement, insurance directive, or internal compliance instruction. The retention period begins only upon the final closure of the file, meaning that all substantive work has been completed, all deliverables have been issued, and no further operational activity is reasonably anticipated. Client files must be retained in a manner that preserves the **full authenticity, completeness, traceability, and admissibility** of the record. This includes all correspondence, notes, assessments, forms, supporting documentation, consent materials, internal memoranda, approvals, and records of substantive action taken on the matter. Where a client file is subject to any dispute, claim, inquiry, regulatory review, or anticipated legal proceeding, the file must be preserved indefinitely until the matter is fully and formally resolved and any associated hold is expressly lifted.

2. Donor Agreements

All **donor agreements**, gift instruments, pledge records, funding acknowledgments, grant-related donor commitments, and associated documentation shall be retained for **ten (10) years**, or for such longer period as may be required by **audit, tax, charitable, accounting, reporting, governance, or donor-restriction requirements**. This retention period reflects the heightened evidentiary, financial, and compliance sensitivity of donor-related records and the organization's obligation to preserve clear proof of donor intent, receipt, restrictions, conditions,

reporting commitments, and administrative treatment of donated funds or in-kind support. Donor agreements must be maintained in a secure and retrievable condition so that the organization can demonstrate, at any time, the **lawful receipt, proper stewardship, and accurate disposition of charitable resources**. No donor agreement may be destroyed, amended, or removed from retention prior to the expiration of the applicable retention period and the completion of any outstanding audit, tax review, compliance review, or donor-related obligation. If the donor agreement is tied to restricted funds, recurring pledges, endowment arrangements, or long-term reporting covenants, the record shall be preserved for the duration necessary to satisfy the **full life cycle of the obligation**.

3. Employee Records

All **employee records** shall be retained for **five (5) years following termination of employment**, unless a longer period is required by applicable employment law, benefits law, tax law, payroll regulation, immigration compliance rules, workplace investigation requirements, litigation hold, insurance claim, or internal disciplinary review. Employee records include, without limitation, personnel files, hiring documents, contracts, evaluations, disciplinary records, payroll-related records, leave documentation, benefits information, training acknowledgments, compliance certifications, and separation records. These records shall be preserved in a manner that safeguards confidentiality while ensuring that the organization can substantiate decisions, employment actions, compensation matters, and compliance obligations if later questioned by an authority, tribunal, auditor, or other competent party. Where an employee record is implicated in a grievance, investigation, dispute, claim, or regulatory examination, the record must be retained for the duration of the matter and not destroyed until all legal or administrative risk has fully ceased.

4. Destruction of Records

Upon expiration of the applicable retention period, records may be destroyed only if they are **not subject to any legal hold, compliance hold, audit hold, investigation, dispute, claim, or other preservation requirement**. Destruction shall be performed using **secure, irreversible, and professionally recognized methods** that render the record incapable of reconstruction or retrieval. Paper records must be destroyed by **cross-cut shredding, pulverization, or equivalent secure destruction methods** performed in a controlled environment. Electronic records and digital media must be destroyed by **secure wiping, cryptographic sanitization, degaussing where appropriate, or physical destruction** of the storage medium when necessary to ensure complete non-recoverability. Destruction shall be conducted in a manner that protects confidentiality, prevents unauthorized access, and eliminates any realistic possibility of recovery, misuse, or disclosure. A **certificate of destruction** or equivalent destruction record shall be created and retained as evidence of lawful disposition, identifying the records destroyed, the date of destruction, the method used, the responsible party, and any applicable approval. **No destruction may occur without documented authorization and verification.**

5. Overriding Legal Hold and Preservation Duty

Notwithstanding any retention schedule stated above, **all records are immediately subject to preservation upon notice or reasonable anticipation of litigation, audit, regulatory inquiry, governmental request, internal investigation, or any other circumstance requiring preservation**. In such cases, the normal destruction timetable is suspended in full to the extent necessary to preserve relevant materials. Employees and responsible officers must comply promptly and in good faith with any preservation directive. Failure to preserve records subject to a hold constitutes a serious compliance breach and may result in internal discipline, legal exposure, and reputational harm to the organization. **Preservation obligations always supersede routine destruction authority.**

6. Governance and Accountability

Records retention and destruction shall be administered under a **controlled governance process** designed to ensure consistency, accountability, and defensibility. The organization may designate responsible personnel to oversee retention schedules, monitor legal and operational requirements, approve destruction when appropriate, and confirm that records are managed in accordance with this policy. Any deviation from the retention rules must be supported by documented legal or compliance justification and authorized by appropriate leadership. The organization shall not permit ad hoc disposal, informal deletion, or undocumented destruction of any record category. **Every retention and destruction decision must be capable of external scrutiny and internal verification.**

V. BREACH NOTIFICATION

ASYLUM RESEARCH & GLOBAL ASSISTANCE maintains a strict and uncompromising incident response standard with respect to any **suspected, attempted, or confirmed unauthorized disclosure**, access, transmission, alteration, loss, or misuse of confidential, protected, personal, operational, or legally regulated information. For purposes of this policy, a breach includes any event that may reasonably be interpreted as compromising the **integrity, confidentiality, availability, or lawful control** of such information, whether the compromise is actual, potential, partial, temporary, or inadvertent.

Any employee, contractor, agent, consultant, or affiliated representative who becomes aware of, suspects, or has reasonable grounds to believe that a breach may have occurred shall **report the matter immediately and without delay** to the **Chief Compliance Officer**. **Immediate reporting is mandatory** and shall not be conditioned upon the completion of internal confirmation, informal verification, remediation, or managerial approval. No individual is authorized to delay escalation on the basis of uncertainty, inconvenience, reputational concern, or assumptions regarding materiality. The obligation to report arises at the moment a credible risk is identified.

The initial incident report shall be complete, factual, and sufficiently detailed to support legal, operational, and forensic review. At a minimum, the report shall identify **what information was disclosed or compromised**, the **identity or category of the recipient, recipient system, or unauthorized party**, the **date, time, and manner of the disclosure**, the

timeline of discovery and escalation, the **scope of the affected records or systems**, the **potential legal, regulatory, contractual, operational, reputational, and security impact**, and the **immediate containment and remediation steps already taken or proposed**. The report shall also include any known or reasonably suspected root cause, whether human error, credential compromise, technical failure, policy violation, malicious conduct, or external intrusion. Where precise facts are not yet available, the report must clearly distinguish **verified facts, reasonable suspicions, and unresolved issues**.

Upon receipt of a report, the **Chief Compliance Officer** shall ensure that a **legal and compliance assessment is initiated within 24 hours**. This assessment shall determine, based on available facts and applicable law, whether the event constitutes a notifiable breach, whether any statutory, regulatory, contractual, donor, partner, client, or data subject obligations are triggered, and whether immediate containment, preservation, escalation, or external consultation is required. The assessment shall be documented contemporaneously and maintained in accordance with the organization's recordkeeping and legal hold obligations. Where the facts indicate a heightened risk of harm, the organization shall act conservatively, expeditiously, and with full regard for the most protective applicable standard.

Where a breach creates a **material risk of harm**, the organization shall notify affected parties **promptly and in accordance with applicable legal requirements**. Such notification shall be accurate, clear, and sufficiently detailed to enable the recipient to understand the nature of the breach, the categories of information involved, the potential consequences, and any measures reasonably necessary to mitigate risk. Notifications shall never minimize, obscure, or selectively omit material facts. The organization's duty is to provide **truthful, timely, and lawful disclosure**, not reputational shielding. Where legally required or operationally prudent, the organization may also notify relevant regulators, supervisory authorities, insurers, contractual counterparties, or other authorized stakeholders.

Where the circumstances indicate or reasonably suggest **criminal conduct**, including theft, fraud, unauthorized access, extortion, identity misuse, cyber intrusion, deliberate sabotage, or intentional unlawful disclosure, the organization shall **contact law enforcement without undue delay**. External reporting to law enforcement shall be coordinated by the Chief Compliance Officer, in consultation with counsel where appropriate, and shall be undertaken in a manner that preserves evidence, protects ongoing investigations, and avoids unnecessary prejudice to affected parties. The organization shall not interfere with, conceal, or compromise any lawful investigation.

All personnel are required to **preserve evidence immediately** upon discovery of a suspected or confirmed breach. This includes preserving emails, logs, devices, files, access records, screenshots, messages, audit trails, and any other information reasonably relevant to the event. No individual may delete, overwrite, alter, conceal, or destroy materials relevant to the incident. Any remediation measures must be implemented in a manner that maintains evidentiary integrity and supports subsequent forensic, legal, and compliance review.

Failure to report a suspected or confirmed breach, delay in escalation, inaccurate reporting, or interference with investigation or remediation constitutes a serious violation of organizational

policy and may result in disciplinary action, termination of affiliation, contractual remedies, and referral to relevant authorities where warranted. **Silence, concealment, and delay are not acceptable responses** to a breach. The organization's standard is one of **immediate accountability, documented action, and strict legal compliance**.

VI. CONSEQUENCES

ARGA maintains a zero-tolerance position toward any unauthorized, reckless, negligent, or self-serving disclosure of confidential, proprietary, operational, client, or internal information. Any breach of this policy undermines institutional trust, compromises security, exposes ARGA and its stakeholders to material harm, and may constitute grounds for immediate disciplinary action, civil recovery, and, where applicable, referral to law enforcement or other competent authorities. **The severity of the response will always be determined by the nature of the conduct, the sensitivity of the information involved, the extent of dissemination, the intent of the responsible individual, the presence of prior violations, and the actual or potential harm caused to ARGA or to any affected party.**

- **Unauthorized disclosure.** Any disclosure of protected information without prior authorization, whether made intentionally, carelessly, verbally, in writing, electronically, by social media, through informal conversation, or by any other means, will be treated as a serious breach of duty. **A first offense will ordinarily result in a written warning and formal documentation in the personnel record.** A second offense, or any repeated pattern of disregard for confidentiality obligations, will result in **suspension**, removal from sensitive assignments, and restriction or revocation of access rights pending further review. A third offense, or any single incident that ARGA determines constitutes a **serious breach**, may result in **immediate termination of employment or contract**, regardless of seniority, role, or prior standing. Where necessary to protect ARGA, its clients, or its partners, ARGA may also impose interim protective measures, including account suspension, device seizure for forensic review, access revocation, and mandatory non-disclosure reminders.

- **Intentional disclosure for personal gain or malicious purpose.** Any deliberate disclosure, sale, transfer, publication, exploitation, or misuse of confidential information for personal advantage, competitive benefit, retaliation, coercion, or any other improper purpose will be treated as an aggravated violation and a profound breach of trust. **Such conduct shall ordinarily result in immediate termination** and may also trigger permanent disqualification from future engagement with ARGA or any affiliated entity. In addition, **ARGA reserves the right to pursue civil remedies, injunctive relief, restitution, and the recovery of all direct and consequential losses**, and, where warranted, to refer the matter for **criminal investigation and prosecution to the fullest extent permitted by applicable law**. No internal relationship, professional standing, seniority, or prior performance history shall mitigate the seriousness of

intentional misconduct of this nature. **Intentional misuse of protected information will be treated as a deliberate ethical and legal violation, not as a mere administrative infraction.**

- **Negligent security practices.** Failure to exercise due care in the handling, storage, transmission, labeling, access control, or disposal of sensitive information will be treated as a material lapse in professional responsibility, even where no malicious intent is shown. Negligence includes, without limitation, leaving confidential documents unsecured, sharing credentials, using unapproved channels, failing to verify recipients, bypassing safeguards, retaining information longer than authorized, or ignoring mandatory security procedures. **Where ARGA determines that the violation resulted from negligence rather than intentional misconduct, the default corrective response shall include mandatory retraining, documented counseling, and placement on a performance improvement plan where appropriate.** Depending on the seriousness of the incident, ARGA may also restrict access privileges, require supervised handling of information, impose temporary suspension, or require written assurances of future compliance. **Repeated negligence will be treated as willful disregard** if the individual continues to ignore clearly communicated requirements after training, notice, or prior correction.

- **Civil liability and recovery of losses.** ARGA expressly reserves the right to seek recovery from responsible individuals or entities for **all losses, damages, costs, liabilities, penalties, remediation expenses, and legal fees** arising from or connected to a breach of this policy, to the fullest extent allowed by law. This includes, where applicable, costs associated with incident response, forensic investigation, containment, client notification, regulatory review, corrective action, reputational harm mitigation, business interruption, and any other direct or foreseeable consequence of the breach. **Civil liability may apply independently of internal disciplinary action**, meaning that termination, suspension, or retraining does not eliminate the possibility of financial claims or other legal proceedings. ARGA may also pursue equitable relief, including orders preventing further disclosure, requiring return or destruction of materials, and compelling cooperation in remediation efforts.

In all cases, ARGA will apply this policy with consistency, seriousness, and documented review, while preserving its full right to determine the appropriate response based on the facts and the gravity of the violation.

No individual may rely on ignorance, convenience, pressure from third parties, or informal practice as a justification for non-compliance. **Confidentiality is a binding obligation, not a discretionary preference**, and any breach will be addressed decisively in defense of ARGA's mission, integrity, and legal interests.

Signed by:

Sergei Khrabrykh

President, Asylum Research & Global Assistance

Date: 18 January 2024