Data Protection and Cybersecurity Policy

Asylum Research & Global Assistance

Preamble

Asylum Research & Global Assistance recognizes that the integrity, confidentiality, availability, and lawful handling of information are not merely administrative concerns, but **fundamental operational obligations** and essential conditions for the lawful, ethical, and effective performance of its mission. In the course of its humanitarian, legal, advisory, research, and administrative activities, the organization necessarily processes highly sensitive personal and organizational data, including but not limited to **client identities, family and dependency information, immigration and asylum records, legal submissions, correspondence, case notes, evidence materials, staff records, contractor information, financial documentation, internal communications, and security-related information**. The disclosure, alteration, loss, misuse, or unauthorized access to such information may result in severe legal, operational, financial, reputational, and, in certain circumstances, physical harm to the individuals concerned. Accordingly, Asylum Research & Global Assistance treats data protection and cybersecurity as **core duties of governance, diligence, and institutional trust**.

This Policy is adopted to establish a comprehensive, binding, and enforceable framework governing the collection, use, storage, transfer, retention, disclosure, protection, and disposal of information processed by or on behalf of Asylum Research & Global Assistance. It applies to all personnel, including employees, officers, directors, consultants, volunteers, contractors, interns, temporary staff, and any third party acting under the organization's authority or accessing its systems, records, or facilities. **No person acting for or on behalf of the organization is exempt from these obligations.** All processing of personal data shall be limited to what is **lawful, fair, necessary, proportionate, and strictly aligned with legitimate organizational purposes**. Data shall not be collected, used, retained, or shared beyond what is required for a defined and legitimate purpose, and no information shall be handled in a manner that undermines the rights, dignity, safety, or lawful interests of any data subject.

This Policy is designed to ensure compliance with applicable international, supranational, and domestic legal frameworks, including, where relevant, the **General Data Protection Regulation (GDPR)**, the **California Consumer Privacy Act (CCPA)**, the **Lei Geral de Proteção de Dados (LGPD)**, the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, and any equivalent or supplementary legal requirements applicable in the jurisdictions in which Asylum Research & Global Assistance operates, receives information, or serves individuals. Where multiple legal regimes apply, the organization shall adopt the **highest practicable standard of protection**, especially where the data concerns vulnerable persons, asylum seekers, refugees, survivors of persecution, victims of violence, or other individuals whose safety, liberty, or legal status may be affected by data misuse. In such

contexts, the organization shall exercise **enhanced care, heightened confidentiality, and strict access control**.

The organization further recognizes that cybersecurity is inseparable from data protection. A lawful data protection framework is incomplete without technical and organizational measures capable of preserving the security of information systems and preventing unauthorized access, unlawful interception, malicious intrusion, ransomware, phishing, social engineering, insider misuse, accidental disclosure, and other cyber threats. Asylum Research & Global Assistance therefore commits to maintaining **risk-based, layered, and continuously reviewed security controls**, including appropriate access governance, authentication safeguards, encryption, secure configuration, logging and monitoring, endpoint protection, secure backup practices, incident response readiness, vulnerability management, and staff awareness measures. Security controls shall be implemented not as a formality, but as a **mandatory institutional safeguard** proportionate to the sensitivity of the information processed and the foreseeable threats faced.

This Policy also establishes the organization's approach to breach management and incident response. Any actual or suspected compromise of personal data, confidential information, or information systems shall be treated with seriousness, urgency, and discipline. The organization shall investigate such events promptly, preserve relevant evidence, assess impact and risk without delay, contain the incident, and determine whether notification or remedial action is required under applicable law, contractual obligation, or internal governance standards. **Failure to report, concealment of incidents, negligent handling of alerts, or retaliation against those who raise concerns is strictly prohibited.** Timely escalation is a duty, not an option.

All processing activities conducted by Asylum Research & Global Assistance shall be guided by the principles of **lawfulness, accountability, necessity, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and transparency**. The organization shall maintain documentation sufficient to demonstrate compliance, shall require appropriate safeguards from processors and partners, and shall review its practices periodically to ensure continued legal and operational adequacy. Where third parties are engaged, they shall be bound by written obligations no less protective than those imposed by this Policy and applicable law. The organization shall not knowingly engage, retain, or tolerate any practice that compromises the confidentiality or lawful handling of protected information.

This Policy expresses a strict institutional commitment to responsible stewardship of information. **Trust, confidentiality, and lawful conduct are mandatory standards, not aspirational values.** Every individual covered by this Policy is expected to act with vigilance, restraint, and professional discipline, and to treat all data entrusted to the organization as information held in confidence, used only for legitimate purposes, and protected with uncompromising seriousness. Any breach of this Policy may result in disciplinary action, contractual remedies, termination of access, referral to competent authorities, or other measures deemed appropriate under applicable law and internal governance requirements.

I. CORE PRINCIPLES

ASYLUM RESEARCH & GLOBAL ASSISTANCE is committed to the highest standards of **lawful, ethical, and accountable data processing**. All handling of personal data shall be governed by the principles set out below, which are not aspirational statements but **mandatory operational standards** applicable to every stage of the data lifecycle, including collection, recording, organization, structuring, storage, use, disclosure, transfer, restriction, deletion, and destruction. These principles shall be interpreted and applied in a manner that protects the **rights, dignity, security, and legitimate expectations** of all individuals whose data is processed by or on behalf of the organization.

1. Lawfulness, Fairness, and Transparency

Personal data shall be processed only where there is a valid and identifiable legal basis and only in a manner that is **lawful, fair, and transparent** to the data subject. The organization shall not engage in any processing that is deceptive, misleading, coercive, abusive, or otherwise inconsistent with the reasonable understanding of the individual concerned. All data processing activities shall be supported by clear, accessible, and meaningful information regarding the nature of the processing, the purposes for which the data is used, the categories of data involved, the legal basis relied upon, the recipients or categories of recipients, and any applicable retention or transfer practices. **Transparency is a duty, not a courtesy**; it requires that data subjects be informed in a way that is intelligible, timely, and sufficiently detailed to enable informed understanding and, where applicable, the exercise of their rights. Any ambiguity shall be resolved in favor of clarity, accountability, and lawful restraint.

2. Purpose Limitation

Personal data shall be collected and processed only for **specified, explicit, and legitimate purposes** that are determined before or at the time of collection. The organization shall not process personal data in a manner incompatible with those purposes, nor shall it repurpose data in a way that exceeds the original lawful scope absent a proper legal basis and appropriate assessment of compatibility. This principle requires operational discipline: every dataset, record, and processing activity must be tied to a clearly articulated objective that is necessary, proportionate, and capable of justification. **Data shall never be collected "just in case" or retained as a matter of convenience**. The organization shall ensure that all personnel understand that expansion of purpose without authority is a serious governance failure and a violation of trust.

3. Data Minimization

The organization shall collect, request, access, and retain only the personal data that is **adequate, relevant, and strictly necessary** for the identified purpose. Excessive collection is incompatible with professional data governance and will not be tolerated. Where a business, legal, or operational objective can be achieved with less information, the lesser amount must be used. Forms, workflows, questionnaires, files, and internal systems shall be designed to avoid unnecessary fields, optional overcollection, speculative requests, and broad data capture.

Necessity is the governing standard: if a data element is not required for a legitimate and defined purpose, it should not be collected. This principle applies equally to manual processing, electronic systems, reporting mechanisms, correspondence, and shared work environments.

4. Accuracy

Personal data shall be kept **accurate, complete, and, where necessary, up to date**. The organization shall take reasonable steps to ensure that inaccurate or misleading data is corrected, supplemented, updated, or deleted without undue delay, having regard to the purpose for which the data is processed. Accuracy is not a passive expectation; it requires active maintenance, verification processes where appropriate, and reliable mechanisms for correction. Where a record is disputed, incomplete, outdated, or potentially erroneous, appropriate controls shall be applied to prevent decisions being made on the basis of defective information. **No person should suffer legal, administrative, operational, or reputational harm because the organization failed to maintain accurate records**. This obligation applies with particular seriousness to data that may affect eligibility, status, rights, access, assessments, or decision-making.

5. Storage Limitation

Personal data shall be retained **only for as long as necessary** to fulfill the purpose for which it was collected, to comply with legal or regulatory obligations, to establish, exercise, or defend legal claims, or to serve another valid and documented retention basis. Retention shall never be indefinite by default. The organization shall maintain retention practices that are purposeful, documented, and periodically reviewed, and shall ensure that data no longer required is securely deleted, anonymized, or otherwise irreversibly disposed of in accordance with approved procedures. **Retention without necessity is a form of risk accumulation** and is inconsistent with professional governance. Where retention is mandated by law, the organization shall limit processing during the retention period to what is strictly required and shall not use retained data for unrelated or expanded purposes.

6. Integrity and Confidentiality

Personal data shall be processed in a manner that ensures **appropriate security, integrity, and confidentiality**, including protection against unauthorized or unlawful processing and against accidental loss, destruction, alteration, disclosure, or access. The organization shall implement technical and organizational measures proportionate to the nature of the data, the context of processing, the risks involved, and the potential impact on individuals. Such measures shall include, where appropriate, access controls, authentication protocols, encryption, secure storage, auditability, least-privilege access, staff training, incident response readiness, vendor oversight, and ongoing security review. **Confidentiality is a core obligation of trust** and must be preserved in all internal and external communications, records handling, and system administration. Any access to personal data must be justified by legitimate need and limited strictly to authorized personnel acting within their defined responsibilities.

7. Accountability and Continuous Compliance

These principles shall be implemented through **documented governance, supervisory oversight, staff responsibility, and demonstrable compliance controls**. Every employee, contractor, partner, and service provider acting on behalf of ASYLUM RESEARCH & GLOBAL ASSISTANCE is expected to comply with these standards without exception. Managers and responsible officers shall ensure that processes, systems, and vendor relationships are designed to support compliance from the outset and maintained throughout the lifecycle of the data. Where uncertainty exists, the organization shall adopt the most privacy-protective and legally defensible course consistent with its obligations. **Moral seriousness, legal precision, and operational discipline are mandatory**, and no business objective may justify disregard for the fundamental principles of lawful data stewardship.

II. DATA CLASSIFICATION

The protection, handling, disclosure, storage, and transmission of information handled by ASYLUM RESEARCH & GLOBAL ASSISTANCE ("ARGA") shall be governed by the following mandatory classification framework. All personnel, contractors, consultants, and any other authorized persons acting on behalf of ARGA shall strictly observe these requirements at all times. **No information may be accessed, shared, retained, transmitted, reproduced, or disclosed except in accordance with its assigned classification level, applicable law, and ARGA authorization.** Any ambiguity regarding classification shall be resolved in favor of the **highest reasonable level of protection**.

A. Confidential (Level 1)

Confidential information constitutes the highest sensitivity category of data handled by ARGA and includes, without limitation, any information the unauthorized disclosure of which could expose an individual, compromise a protection claim, prejudice legal proceedings, create personal risk, or materially damage ARGA's mission, operations, or legal integrity. This category includes, but is not limited to, **personal data** such as full names, aliases, dates of birth, home and mailing addresses, telephone numbers, email addresses, passport numbers, identity document numbers, immigration identifiers, biometric information, family composition, location data, case histories, interview notes, affidavits, medical records, vulnerability assessments, financial information, bank account details, donation records linked to individuals, asylum narratives, legal strategies, supporting evidence, litigation plans, witness statements, and any other material of a sensitive, private, privileged, or legally protected character.

Access to Confidential information is strictly limited to specifically authorized personnel with a demonstrable operational need to know. Such access shall be granted only where necessary for the legitimate performance of assigned duties and only to the minimum extent required. **Confidential information shall never be disclosed to any unauthorized person, entity, or platform, whether intentionally, negligently, or by omission.** This prohibition applies equally to oral disclosure, written disclosure, digital transfer, screen visibility,

printed documents, cloud storage, messaging applications, informal discussion, and any indirect form of exposure.

Confidential data shall be protected by robust technical, administrative, and physical safeguards. At a minimum, this includes **encryption at rest and in transit**, strong access controls, role-based permissions, password protection, multifactor authentication where available, secure storage environments, restricted device access, logging and monitoring of access activity, and secure deletion protocols where retention is no longer required. Printed or physical materials containing Confidential data shall be stored in secure, access-controlled locations and shall not be left unattended in open offices, shared spaces, or public areas.

Transmission of Confidential information shall occur only through approved secure channels. Personnel shall not use personal email accounts, unsecured messaging applications, unapproved cloud services, or other informal platforms for the transfer of Confidential information. Where transmission is unavoidable, the sender shall ensure that the recipient is authorized, the content is minimized, the file is protected, and the transmission method affords adequate security. **Any suspected compromise, misdirection, unauthorized access, loss, or accidental disclosure of Confidential data shall be treated as a critical incident and reported immediately in accordance with ARGA incident response procedures.**

B. Internal (Level 2)

Internal information comprises non-public operational, administrative, and organizational material intended solely for use within ARGA and its authorized working structure. This category includes, without limitation, **staff directories, internal policies, operational procedures, internal templates, workflow instructions, internal memoranda, training materials, non-public organizational charts, internal communications, scheduling information, and other information not intended for public circulation but which does not rise to the level of Confidential sensitivity.**

Access to Internal information shall be limited to **ARGA personnel and other expressly authorized individuals** who require such information for legitimate organizational purposes. **Internal data shall not be shared outside ARGA unless prior authorization has been granted by competent management or disclosure is otherwise required by law.** Even where disclosure is permitted, the information shall be limited to the minimum necessary scope and handled in a manner consistent with ARGA's confidentiality obligations.

Standard protective measures shall apply to Internal information, including reasonable access controls, secure storage, controlled distribution, and appropriate retention practices. While Internal information may not require the same degree of protection as Confidential data, it remains subject to the duty of care owed by all ARGA personnel. Accordingly, such information shall not be casually disclosed, circulated without purpose, or used in a manner that could undermine operational integrity, internal governance, staff confidentiality, or institutional security. **Personnel are responsible for ensuring that Internal information remains within approved channels and is not exposed through carelessness, convenience, or misuse.**

Where Internal information contains operational details that, if widely known, could create security, reputational, or organizational risk, ARGA may apply enhanced controls notwithstanding its default classification level. **The classification of information depends not merely on form, but on context, content, and foreseeable harm arising from disclosure.**

C. Public (Level 3)

Public information consists of material expressly intended for unrestricted external access and distribution. This includes, without limitation, **published reports, public-facing website content, press releases, public announcements, approved informational materials, and any other content that ARGA has formally authorized for public release.** Public classification shall apply only where information has been reviewed and expressly designated for public dissemination by ARGA through appropriate authorization channels.

Public information may be accessed and distributed without restriction, provided that it is reproduced accurately and not presented in a misleading, incomplete, defamatory, or unauthorized manner. **Public availability does not authorize alteration, misrepresentation, selective quotation, or the removal of contextual safeguards that could distort meaning or compromise ARGA's integrity.** Where necessary, ARGA may impose citation, attribution, branding, or usage requirements to preserve authenticity and prevent misuse.

Information shall not be classified as Public merely because it is widely known, informally shared, or accessible through external sources. **Only information affirmatively approved for public release shall be treated as Public under this policy.** Any information not expressly released by ARGA shall remain subject to the applicable internal or confidential protections corresponding to its actual sensitivity.

Classification is a continuing obligation, not a one-time label. All personnel are required to assess information carefully, apply the appropriate classification conservatively, and re-evaluate classification whenever the content, context, intended audience, or risk profile changes. **Misclassification, negligent handling, or unauthorized disclosure of any category of data constitutes a serious breach of ARGA policy and may result in disciplinary action, contractual consequences, reporting obligations, and any other measures permitted by law or organizational authority.**

III. TECHNICAL SAFEGUARDS

A. Encryption

All personal data, confidential business records, client materials, investigative information, operational documentation, and any other information designated as sensitive or restricted shall be protected by **strong cryptographic controls** that are commensurate with the nature of the data, the volume of processing, the sensitivity of the use case, and the foreseeable risks of unauthorized access, disclosure, alteration, or destruction. **Encryption is not optional**; it is a

foundational control and an essential requirement for the lawful, secure, and professionally responsible handling of information within ASYLUM RESEARCH & GLOBAL ASSISTANCE.

For **data at rest**, the organization shall apply **AES-256 encryption or an equally robust industry-standard algorithm approved by competent technical authority** to all databases, file servers, endpoint storage, backup repositories, archives, removable media, and cloud-based storage environments where sensitive data is stored or may reasonably be reconstructed. Encryption keys shall be generated, stored, rotated, protected, and retired under a formal key management framework designed to prevent unauthorized disclosure, compromise, or misuse. Access to encryption keys shall be restricted to authorized systems and personnel strictly on a **least-privilege basis**, and key material shall never be embedded in source code, unsecured configuration files, shared credentials, or unprotected scripts. The organization shall ensure that encryption remains effective not merely in design, but in operational practice, including during replication, synchronization, migration, and retention processes.

For **data in transit**, the organization shall require **TLS 1.2 or higher**, with a preference for the most secure and current protocol versions and cipher suites reasonably available and operationally compatible. All web-based interfaces, internal communications channels, application programming interfaces, remote administrative sessions, virtual private network connections, and other transmission pathways used to move sensitive data shall be protected against interception, tampering, replay, downgrade attacks, and unauthorized disclosure. Plaintext transmission of sensitive information over public or untrusted networks is prohibited unless a documented exceptional necessity exists and an approved compensating control is implemented. Certificate management shall be governed by strict verification, renewal, revocation, and trust-chain validation procedures to ensure the integrity of encrypted communications.

Where sensitive information is transmitted by electronic mail or equivalent messaging systems, **end-to-end encryption shall be used whenever technically feasible and operationally appropriate**, particularly where the content contains personal data, privileged material, legal records, investigative findings, security-sensitive intelligence, or any other information that could expose individuals, clients, or the organization to material harm if compromised. The organization shall implement controls to reduce the risk of accidental misdirection, unauthorized forwarding, insecure attachment handling, and exposure through third-party mail systems. Encryption requirements shall be reinforced through user awareness, technical enforcement, and supervisory oversight, and no employee may circumvent such protections for convenience, speed, or informal practice.

B. Access Control

Access to systems, networks, databases, applications, cloud services, records, and administrative tools shall be governed by **strict access control principles** designed to ensure that only duly authorized persons can view, process, modify, export, or otherwise interact with protected information. **The guiding rule shall be necessity, not preference**: access must be granted only where required for a legitimate business function, and never more broadly than is essential to accomplish that function safely and lawfully.

Multi-factor authentication (MFA) shall be mandatory for all staff, contractors, consultants, temporary workers, and any other persons who access organizational systems, with heightened protections for privileged, supervisory, administrative, and remote-access accounts. MFA shall be required for authentication to core systems, email, cloud portals, privileged command interfaces, remote access services, and any environment containing sensitive or regulated information. Passwords alone shall never constitute adequate protection for privileged access. Privileged credentials shall be subject to enhanced scrutiny, stronger identity verification, and where appropriate, step-up authentication, session restrictions, and device trust requirements.

The organization shall implement **role-based access control (RBAC)** under a **least privilege principle** that is enforced by design, reviewed by management, and validated through periodic audit. Access rights shall correspond to documented job functions, operational necessity, and approval by appropriate authority. Standing access shall be avoided wherever reasonably possible, and elevated permissions shall be limited in scope, duration, and purpose. Shared accounts are prohibited except where expressly justified, formally approved, technically controlled, and continuously monitored. Separation of duties shall be applied to sensitive workflows so that no single individual can unilaterally authorize, execute, and conceal critical actions that could affect data integrity, confidentiality, or operational security.

Access rights shall be reviewed **at least quarterly**, and more frequently where the sensitivity of the environment warrants it. Such reviews shall verify that permissions remain accurate, justified, and proportionate to current responsibilities. **Immediate removal or suspension of access shall occur upon termination of employment, contract expiration, reassignment, disciplinary removal, or any other event that extinguishes the lawful basis for access**. Where there is any credible indication of risk, access shall be reduced or revoked without delay, and credentials, tokens, certificates, device trust relationships, and other authentication artifacts shall be invalidated promptly. Delayed deprovisioning is unacceptable where it creates avoidable exposure.

All access attempts, whether successful or unsuccessful, shall generate **audit logs sufficient to reconstruct who accessed what, when, from where, by which method, and for what administrative or operational purpose**. Logs shall be protected against alteration, deletion, and unauthorized disclosure, and shall be retained for **no less than 12 months**, or longer where legal obligation, contractual requirement, incident response needs, or regulatory expectation requires. Logging controls shall extend to privileged activity, configuration changes, authentication events, data exports, permission changes, failed logins, anomalous access patterns, and other events material to security oversight. The existence of logs is not, by itself, sufficient; they must be reviewable, actionable, and preserved in a manner that supports accountability, forensic inquiry, and compliance verification.

C. Network Security

The organization shall maintain a **defense-in-depth network security architecture** designed to detect, block, contain, and rapidly respond to malicious activity, unauthorized traffic, misconfiguration, and exploitation attempts. Network security shall be treated as a continuous operational obligation rather than a static technical feature. Systems shall be segmented and

protected in a manner appropriate to their sensitivity, exposure, and role in organizational operations.

Firewalls, intrusion detection systems, and intrusion prevention systems (IDS/IPS) shall be deployed at appropriate network boundaries and internally where risk warrants, with rulesets configured to enforce approved communications, limit unnecessary exposure, and identify or prevent suspicious behavior. Firewall rules shall be formally documented, periodically reviewed, and restricted to the minimum necessary traffic required for business operations. Any exception to standard network restrictions shall require documented justification and supervisory approval. IDS/IPS signatures, policies, and behavioral detection rules shall be maintained in a timely manner so that the organization can identify known attack patterns, abnormal lateral movement, brute-force attempts, command-and-control indicators, and other threats commonly associated with compromise.

The organization shall conduct **regular vulnerability assessments at least quarterly** and **penetration testing at least annually**, with additional testing when significant architectural changes, emerging threats, major incidents, or high-risk exposures justify immediate re-evaluation. Vulnerability assessments shall cover externally facing assets, internal systems, cloud workloads, applications, authentication layers, remote access services, and other material attack surfaces. Identified vulnerabilities shall be risk-ranked, remediated according to severity, and tracked to closure under formal accountability. Exploitable weaknesses shall not be left unresolved by inertia, uncertainty, or administrative delay where reasonable remediation is available.

Critical security patches and updates shall be deployed within 30 days of release, and sooner where a vulnerability presents active exploitation risk, widely known abuse potential, or severe operational impact. Where patching cannot occur within the required period due to technical constraints or business continuity concerns, the organization shall implement documented compensating controls, including but not limited to isolation, access restriction, additional monitoring, virtual patching, or temporary service suspension. Unsupported software, end-of-life systems, and unpatched legacy environments shall not be retained without formal risk acceptance at the appropriate level of authority and a documented remediation plan. The organization shall act with urgency, discipline, and technical competence to prevent avoidable exposure from becoming institutionalized negligence.

D. Backup & Disaster Recovery

The organization shall maintain a **resilient backup and disaster recovery framework** designed to preserve the integrity, availability, and recoverability of critical information and operational capability in the event of cyber incident, human error, system failure, natural disaster, infrastructure outage, sabotage, or other disruptive event. Backups are not a mere archival convenience; they are a core control necessary to ensure continuity, restore trust, and prevent irreversible loss.

Backups shall be performed on a **daily incremental basis** and a **weekly full basis**, or at a frequency more protective than this minimum where the business function, risk profile, or data volatility requires. Backup processes shall be automated where feasible, monitored for success or

failure, and subject to exception reporting so that missed jobs, corruption, and retention issues are identified promptly. Backup data shall include the systems, configurations, logs, and metadata necessary to support meaningful restoration, not merely isolated files. The organization shall ensure that backup strategies are aligned with data classification, retention obligations, and recovery priorities, so that critical functions can be restored in a coherent and operationally useful manner.

Backup copies shall be stored in **at least two geographically separated locations** to reduce the likelihood that a single event, whether physical, environmental, or cyber-related, can destroy both primary and recovery data. Where cloud services are used, the organization shall confirm that backup arrangements provide genuine logical and geographic separation, not merely nominal replication within the same failure domain. Backup repositories shall themselves be protected by strong access controls, encryption, immutability or equivalent anti-tamper safeguards where feasible, and monitoring designed to detect unauthorized deletion, encryption by malware, or retention failures. The organization shall not rely on backups that can be readily altered, silently compromised, or deleted by the same compromised credentials used to attack the primary environment.

The organization sets a **Recovery Time Objective (RTO) of 4 hours** and a **Recovery Point Objective (RPO) of 1 hour** for critical services, subject to the technical capabilities and risk classification of the relevant system. These objectives are mandatory operational commitments and shall inform architecture, monitoring, staffing, redundancy, and contingency planning. Recovery procedures shall be sufficiently documented, rehearsed, and resourced so that restoration is feasible under pressure and not merely theoretical on paper. Systems and data with higher criticality shall receive proportionately stronger continuity controls, including prioritized restoration order, dependency mapping, and contingency communications planning.

A formal **disaster recovery drill shall be conducted annually at minimum**, and more frequently where the organization's risk profile, system changes, or incident history justify it. Drills shall test not only technical restoration, but also decision-making, communications, escalation pathways, vendor coordination, and the practical ability of personnel to execute recovery procedures under realistic conditions. Findings from each drill shall be documented, analyzed, and translated into corrective action with accountable owners and deadlines. Recovery planning that is not tested is not reliable; and recovery capability that cannot be demonstrated is not a control worthy of professional reliance.

General Principle

All technical safeguards described above shall be implemented, maintained, monitored, and improved as part of a **continuous security governance framework**. Technical safeguards must be supported by competent oversight, documented procedures, staff accountability, and periodic reassessment. **Security shall be proactive, preventive, and uncompromising**. Where risk cannot be eliminated, it must be reduced to the lowest practicable level by lawful, technically sound, and professionally defensible means.

IV. ORGANIZATIONAL CONTROLS

A. Data Processing Agreements (DPAs)

ASYLUM RESEARCH & GLOBAL ASSISTANCE shall ensure that no third party processes personal data on its behalf unless and until a **written, duly executed Data Processing Agreement ("DPA")** is in place and has been reviewed for full alignment with **GDPR requirements**, applicable data protection laws, and the internal compliance standards of the organization. This requirement applies to **all data processors without exception**, including, but not limited to, cloud infrastructure providers, software-as-a-service vendors, hosting providers, payroll contractors, customer support platforms, archival services, analytics providers, and any outsourcing partner that may access, store, transmit, retrieve, or otherwise handle personal data in the course of service delivery. **No processing relationship may be permitted on the basis of informal assurances, standard commercial terms alone, or implied consent.**

Each DPA must unequivocally define the **subject matter, duration, nature, and purpose of processing**, the **types of personal data involved**, the **categories of data subjects affected**, and the **documented instructions** issued by ASYLUM RESEARCH & GLOBAL ASSISTANCE as controller or, where applicable, a processor acting on behalf of another controller. The agreement must impose clear and enforceable obligations on the processor to process personal data **solely for documented instructions**, to maintain **strict confidentiality**, to implement **appropriate technical and organizational measures**, to ensure that any person authorized to process personal data is bound by equivalent confidentiality obligations, and to provide all assistance reasonably required to enable compliance with **data subject rights, security obligations, breach notification requirements, DPIA support, and supervisory authority inquiries**. The DPA must further require the processor to maintain complete and accurate records of processing activities where legally applicable and to make such records available upon request for compliance verification.

A processor may engage a sub-processor only where **prior written authorization** has been expressly granted by ASYLUM RESEARCH & GLOBAL ASSISTANCE. Such authorization shall be granted either on a specific basis or through a properly defined general authorization mechanism, but in all cases the processor must provide **advance notice of any intended addition or replacement of a sub-processor** with sufficient detail to allow meaningful review and, where necessary, objection. ASYLUM RESEARCH & GLOBAL ASSISTANCE shall retain the right to **approve, condition, restrict, or refuse** any proposed sub-processing arrangement where the proposed engagement introduces unacceptable risk, weakens legal safeguards, or fails to meet the organization's security and compliance expectations. The processor must impose on every sub-processor **the same or materially equivalent data protection obligations** as those contained in the principal DPA, and the processor shall remain **fully liable** for the acts and omissions of its sub-processors as if they were its own.

Where a change in sub-processor arrangement materially affects the manner in which personal data is processed, the nature of the security environment, or the jurisdictional exposure of the data, **advance notification to affected data subjects shall be made where legally**

required and operationally appropriate, and internal compliance review shall be completed before the change takes effect. In all cases, ASYLUM RESEARCH & GLOBAL ASSISTANCE shall maintain the authority to require **supplementary contractual safeguards**, enhanced monitoring, or termination of the service relationship where the risk profile changes materially. Each DPA must also include provisions governing **security incident and personal data breach notification**, **audit and inspection rights**, **cooperation with regulators**, **cross-border transfer mechanisms where applicable**, **data return or certified deletion upon termination**, and **immediate cessation of processing upon unlawful or unauthorized instruction**. Any processor that is unwilling or unable to meet these standards shall be deemed **unfit for engagement**.

B. Privacy by Design

Privacy by Design is a mandatory operating principle, not a discretionary enhancement. ASYLUM RESEARCH & GLOBAL ASSISTANCE shall ensure that privacy and data protection considerations are embedded from the earliest stages of planning, procurement, architecture, development, testing, deployment, and operational maintenance of any new system, workflow, product, service, or process that involves personal data. **Data protection must be engineered into the lifecycle of operations, not retrofitted after implementation, and never treated as a mere compliance formality.** Every relevant initiative shall be assessed for necessity, proportionality, lawful basis, data minimization, retention limitations, transparency, security, and the rights and freedoms of data subjects before implementation is approved.

A **Data Protection Impact Assessment ("DPIA")** shall be conducted whenever a new or materially changed system, process, or technology is likely to result in a high risk to the rights and freedoms of individuals, or whenever the nature, scope, context, or purpose of processing creates heightened privacy, security, or ethical sensitivity. Such assessment shall not be superficial or ceremonial; it must be a **substantive, evidence-based examination** of the processing activity, including the categories of data collected, the justification for collection, the necessity of each processing step, the potential impact on individuals, the likelihood and severity of harm, the robustness of security safeguards, and the feasibility of alternative, less intrusive design choices. Where residual risk remains high after mitigation, escalation to appropriate governance oversight shall occur prior to deployment, and processing shall not commence until the risk is formally reviewed and accepted by the competent decision-makers in accordance with the organization's risk governance framework.

The privacy-by-design methodology shall require, as a matter of default, **data minimization**, **purpose limitation**, **restricted access**, **least-privilege architecture**, **strong authentication**, **encryption in transit and at rest where appropriate**, **secure logging**, **segregation of environments**, **pseudonymization or anonymization where feasible**, and **strict retention controls** ensuring that personal data is not retained longer than necessary for the legitimate purpose identified. Default system settings must favor the **highest reasonable level of privacy protection**, and any exception must be expressly justified, documented, approved, and periodically revalidated. Development and procurement teams shall

not proceed on the assumption that security or privacy can be corrected later; rather, they must demonstrate that privacy controls have been incorporated at the design stage and verified before release. This includes privacy review of vendor tools, software integrations, APIs, and automated decision-making features, with special scrutiny applied to any processing involving sensitive data, vulnerable persons, cross-border data flows, or large-scale monitoring.

The organization shall maintain formal gating procedures to ensure that **no new processing activity is launched without documented privacy review**, and that any material modification to an existing system triggers reassessment. Compliance is not satisfied by nominal consideration alone; it requires **traceable evidence of design choices, risk acceptance, mitigation measures, and accountability assignments**. In this regard, ASYLUM RESEARCH & GLOBAL ASSISTANCE shall uphold a strict standard of diligence, recognizing that privacy failures are not merely operational defects but **breaches of trust, legality, and institutional integrity**.

C. Staff Training

No privacy program can be effective without a trained workforce. ASYLUM RESEARCH & GLOBAL ASSISTANCE shall require **mandatory data protection training for all personnel within 30 days of hire**, without exception for seniority, function, contractor status, or geographic location where the individual has access to organizational systems or personal data. The initial training shall be no shorter than **two hours**, and shall cover the core legal and operational obligations relevant to the organization, including **lawful processing principles, confidentiality expectations, data subject rights, secure handling practices, incident reporting duties, phishing and social engineering awareness, acceptable use requirements, retention discipline, and the consequences of non-compliance**. This training must be completed before the employee is permitted to handle personal data independently, where role sensitivity so requires. Completion shall be recorded, monitored, and retained as part of the organization's compliance evidence.

In addition to the initial onboarding requirement, all personnel shall complete **annual refresher training of at least one hour** to ensure continuing awareness of legal obligations, policy updates, procedural changes, regulatory developments, and emerging threats. Refresher training must not be generic or perfunctory; it shall be **role-relevant, practical, and risk-informed**, with tailored content for personnel whose responsibilities involve access to sensitive data, external communications, security administration, vendor management, human resources, legal review, research activities, or systems development. Where operational changes, incidents, audit findings, or regulatory updates reveal a specific weakness in staff understanding, additional targeted training shall be required promptly and without delay.

To reinforce behavioral resilience and incident readiness, ASYLUM RESEARCH & GLOBAL ASSISTANCE shall conduct **quarterly phishing simulation tests** for relevant personnel. These simulations shall be designed to assess genuine susceptibility to deceptive messages, credential compromise attempts, malicious links, attachment-based attacks, and impersonation tactics. Results shall be **documented, analyzed, and retained**, and the organization shall use the findings to identify recurring vulnerability patterns, refine training content, and deploy

targeted remedial instruction to individuals, teams, or departments that exhibit elevated risk. A punitive mindset is not the primary objective; however, **accountability is non-negotiable**. Repeated failure to complete mandatory training, chronic inability to recognize obvious threats, or disregard of established privacy procedures may result in escalated supervision, restricted access, disciplinary action, or other measures deemed necessary to protect data, systems, and affected individuals.

Training records shall be maintained in a manner sufficient to demonstrate compliance, including the date of completion, duration, attendance, assessment outcomes where applicable, and evidence of remedial follow-up. The organization shall periodically review training effectiveness through metrics, audit outcomes, incident trends, and simulation performance. Where weaknesses are identified, the curriculum shall be adjusted immediately. **Training is not a ceremonial exercise; it is a core control mechanism, a governance obligation, and a direct safeguard against unlawful, careless, or negligent handling of personal data.**

V. INCIDENT MANAGEMENT

A. Breach Notification

ASYLUM RESEARCH & GLOBAL ASSISTANCE shall maintain a rigorous, time-bound, and evidence-preserving incident management process to ensure that any actual, suspected, or reasonably foreseeable security incident, including any **personal data breach**, is identified, contained, assessed, escalated, and reported in a manner consistent with applicable law, regulatory obligations, contractual commitments, and the Organization's duty to act with **promptness, integrity, and uncompromising diligence**. For purposes of this Policy, a breach shall be understood broadly to include any event that results in, or is reasonably capable of resulting in, **unauthorized access, disclosure, alteration, loss, destruction, unavailability, or compromise of protected information, systems, or assets**. The Organization shall treat the first indication of an incident as legally significant, and no employee, contractor, vendor, or agent may delay escalation on the basis of incomplete facts, assumptions of low impact, or an expectation that the matter may resolve itself without intervention.

Upon discovery of any actual or suspected incident, the matter shall be reported to the **Chief Information Security Officer (CISO) within one (1) hour** of discovery or of reasonable suspicion, whichever occurs first. Discovery shall include any event observed directly by personnel, identified through monitoring tools, raised by a third party, reported by a data subject, or otherwise brought to the attention of the Organization in circumstances that would cause a prudent professional to conclude that a security event may have occurred. The initial report must include, to the extent known at that time, the nature of the incident, the systems or data potentially affected, the date and time of discovery, the source of the report, the immediate containment measures taken, and any known indicators of compromise. The obligation to escalate within one hour is mandatory and non-discretionary; it exists precisely because early failures in reporting frequently magnify operational harm, legal exposure, reputational damage, and the risk of regulatory non-compliance.

The **CISO**, or the designated incident response authority acting under the CISO's supervision, shall ensure that an **initial assessment is completed within twenty-four (24) hours** of discovery. This assessment shall determine, with disciplined and documented reasoning, whether the event constitutes a reportable breach or a security incident requiring further investigation, whether the incident is ongoing, whether containment or eradication steps are required, and whether the incident creates a risk to the rights and freedoms of individuals or other legally protected interests. The assessment shall be based on the best information reasonably available at the time and shall not be deferred merely because a forensic investigation remains incomplete. Where uncertainty exists, the Organization shall apply a **precautionary approach**, prioritizing the protection of individuals, the integrity of systems, and the fulfillment of legal duties over operational convenience.

Where the assessment indicates that the breach is **likely to result in a risk** to individuals, the Organization shall notify the relevant regulators or supervisory authorities **within seventy-two (72) hours** of becoming aware of the breach, unless a shorter period is required by applicable law or contract. If the notification cannot be made within that timeframe, the Organization shall provide the notification as soon as practicable and shall document the reasons for any delay in full, with contemporaneous evidence supporting the factual and legal basis for the timing. Regulatory notifications shall be accurate, complete to the extent possible at the time of submission, and updated without delay as further material facts become known. The Organization shall not withhold or soften material information for reasons of reputational management, operational sensitivity, or convenience; **truthfulness, completeness, and timeliness** shall govern all communications with public authorities.

Where the breach is **confirmed to present a high risk** to the rights, freedoms, safety, confidentiality, or lawful interests of affected data subjects, those individuals shall be notified **without undue delay**. Such notice shall be drafted in clear, intelligible, and direct language and shall describe, where appropriate and legally permissible, the nature of the breach, the categories of data or information involved, the likely consequences, the measures taken or proposed by the Organization to address the breach, and the steps the affected individuals can take to protect themselves. The Organization shall ensure that notification is not diluted by technical jargon, vague reassurance, or incomplete characterization of risk. If direct notification is not legally required or is impossible under the circumstances, the Organization shall consider whether alternative protective measures, including public communication or substitute notice, are required by law or appropriate as a matter of prudence and moral responsibility.

In every case, the Organization shall maintain a comprehensive **incident log** capturing the chronology of events, the decision-making process, the persons involved, the factual basis for each major determination, all containment and remediation actions taken, all notices issued, and any coordination with external counsel, forensic experts, insurers, regulators, or law enforcement. The incident log shall be maintained in a manner that preserves evidentiary integrity and supports internal review, regulatory inquiry, and, where necessary, litigation defense. Upon closure of the incident, the Organization shall conduct a formal **lessons learned review** to identify root causes, control failures, response delays, training gaps, contractual weaknesses, and opportunities for improvement. Corrective actions arising from that review shall

be assigned, tracked, and verified to completion, and may include policy revision, technical hardening, vendor remediation, staff retraining, disciplinary measures, or enhanced oversight.

No incident shall be treated as routine, excusable, or merely administrative when it has the potential to compromise trust, confidentiality, legal compliance, or the dignity and security of those whose information the Organization holds. The Organization shall respond with **speed, accuracy, restraint, accountability, and full documentary discipline**, reflecting its commitment to lawful conduct, ethical rigor, and the highest standards of professional stewardship.

VI. DATA SUBJECT RIGHTS

ASYLUM RESEARCH & GLOBAL ASSISTANCE recognizes that the protection of personal data is inseparable from the protection of individual dignity, autonomy, and lawful treatment. Accordingly, every data subject whose personal data is collected, stored, used, disclosed, transferred, or otherwise processed by or on behalf of the organization shall be afforded the full measure of rights guaranteed under applicable data protection and privacy laws. These rights are not symbolic. They are **operationally enforceable**, **legally binding**, and are administered with strict adherence to principles of **lawfulness**, **fairness**, **transparency**, **data minimization**, **purpose limitation**, **accuracy**, **storage limitation**, **integrity**, **confidentiality**, and **accountability**.

Requests submitted by data subjects shall be handled with seriousness, urgency, and procedural discipline. The organization will not unreasonably delay, obstruct, dilute, or ignore any properly submitted request. For security and legal compliance purposes, the organization may require **reasonable identity verification** before disclosing personal data or implementing requested changes, particularly where the request concerns sensitive records, third-party information, or data that, if improperly released, could compromise the rights and freedoms of others. Where a request is complex, unusually broad, or legally constrained, the organization may extend the response period to the extent permitted by applicable law, provided that the data subject is informed in a timely and transparent manner. Unless otherwise required by law, the organization shall respond **within 30 days** of receipt of a valid request.

Data subjects are entitled to the following rights:

- **Right of access**: The data subject may request confirmation as to whether personal data concerning them is being processed and, where applicable, obtain a copy of such data. The response shall, to the extent required by law, include a meaningful description of the categories of data held, the purposes of processing, the recipients or categories of recipients, the retention logic applied, and any other information necessary to ensure **full and intelligible transparency**. Access shall be granted in a manner that is clear, complete, and not misleading, so that the individual may understand not merely that data exists, but **how and why it is used**.
- **Right to rectification**: The data subject may request the correction of inaccurate, incomplete, outdated, or misleading personal data. Where a request is substantiated, the organization shall take prompt and effective action to correct the record and, where

appropriate, to propagate the correction to relevant processors or recipients, insofar as such action is legally required and operationally feasible. The maintenance of inaccurate data is incompatible with lawful processing; accordingly, ASYLUM RESEARCH & GLOBAL ASSISTANCE treats accuracy as a **mandatory compliance obligation**, not a discretionary courtesy.

- **Right to erasure ("right to be forgotten")**: The data subject may request deletion of personal data where one of the applicable legal grounds for erasure is present. Such requests shall be honored **unless retention is required or otherwise justified by law**, including, where applicable, compliance with statutory recordkeeping obligations, defense of legal claims, fraud prevention, safeguarding of rights and security interests, or other legally recognized grounds for continued processing. Erasure, where granted, shall be implemented with due regard to technical and organizational feasibility, including deletion from active systems and, where appropriate, restriction of further dissemination. The organization shall not retain personal data beyond what is **strictly necessary and legally defensible**.
- **Right to restrict processing**: The data subject may request that the processing of their personal data be limited in circumstances recognized by law, including where accuracy is contested, where processing is unlawful but erasure is not requested, where data is no longer needed for the original purpose but must be preserved for legal reasons, or where the data subject has objected and verification is pending. During a valid restriction period, the organization shall ensure that the affected data is **safeguarded against further use**, except for storage, compliance, or other expressly permitted operations under applicable law. Restriction is treated as a serious protective measure, not as an administrative formality.
- **Right to data portability**: Where required by applicable law, the data subject may request that personal data provided to the organization be exported in a **structured, commonly used, machine-readable, and interoperable format**, and, where technically feasible and legally permissible, transmitted to another controller upon request. This right applies only to the extent recognized by law and shall not prejudice the rights of others, the security of systems, or the confidentiality of protected information. ASYLUM RESEARCH & GLOBAL ASSISTANCE will implement portability requests with the objective of ensuring **practical transferability without compromising legal integrity**.

For all privacy-related inquiries, objections, or requests relating to the exercise of any data subject right, the organization maintains a dedicated Data Protection Officer. Communications may be directed to **dpo@arga.world**. The Data Protection Officer serves as the designated point of contact for the administration of rights requests, the assessment of legal grounds, the coordination of internal compliance measures, and the oversight of privacy governance. All submissions are reviewed under a framework of **strict confidentiality**, **documented accountability**, and **non-retaliatory treatment**.

Nothing in this section shall be construed to diminish or waive any right available to the data subject under applicable law. Where a request is denied in whole or in part, the data subject will be informed of the reason for the decision to the extent legally permissible, together with any available avenues for review, escalation, or complaint. **ASYLUM RESEARCH & GLOBAL ASSISTANCE is committed to lawful, transparent, and ethically uncompromising data governance**, and to the principle that personal data shall never be treated as a matter of convenience, but only as a matter of **legal responsibility and disciplined stewardship**.

Signed by:

Sergei Khrabrykh

President, Asylum Research & Global Assistance

Date: 18 January 2024