Source Classification Policy

Department: Evidence Intake & Verification Desk
Policy ID: EIV-02
Version: 1.0
Effective Date: Upon Publication

1. Policy Title

Source Classification Policy

2. Authority & Legal Standing

2.1 **Binding Instrument.**
This Source Classification Policy (“Policy”) is a binding operational and contractual instrument governing the classification, labelling, handling constraints, and admissibility-routing of any information, data, files, documents, statements, communications, artefacts, or other materials provided to the Organisation (“Submissions”).

2.2 **Condition of Processing; Classification as Mandatory Gate.**
No Submission may proceed beyond intake screening into any internal handling pathway unless it has been assigned a source classification under this Policy. Source classification is a mandatory gate that conditions all downstream handling, including eligibility determination, containment, verification requirements, investigatory routing, analytical use constraints, archival treatment, and publication suitability.

2.3 **Assent Requirement.**
Engagement with the Organisation in any form—including but not limited to commissioning investigations, submitting materials, requesting assessment, or interacting with Organisation intake systems—constitutes acceptance of this Policy upon completion of an acknowledgement step (“Assent”), captured by clickwrap/portal acknowledgement, written confirmation, or signed engagement instrument referencing the Policy title, ID, and version.

2.4 **Assent Evidence and Auditability.**
The Organisation maintains auditable records evidencing Assent, classification assignment, and classification changes (if any), including timestamps, channel identifiers, and submission identifiers, sufficient to demonstrate procedural compliance in judicial, regulatory, arbitral, and oversight contexts.

2.5 **Court and Regulatory Reliance.**
This Policy is drafted to be relied upon as evidence of due process controls, provenance discipline, bias risk containment, and defensible procedural treatment of sources.

3. Purpose

3.1 **Primary Objective.**
The purpose of this Policy is to ensure that every Submission is systematically classified according to its source characteristics and provenance attributes, enabling consistent, defensible handling that prevents unlawful processing, unreliable inference, scope contamination, and biased or malicious targeting.

3.2 **Risk Containment Objective.**
This Policy exists to prevent, at a structural level:
a) the mixing of incompatible source types;
b) the elevation of unverified material into investigative or analytical truth;
c) the laundering of illegally obtained or coercively produced material into legitimacy;
d) the ingestion of manipulated, synthetic, or misattributed material without safeguards;
e) the misuse of open-source data to infer personal wrongdoing without procedural controls.

3.3 **Non-Determination.**
Source classification is a procedural control. It does not determine truth, falsity, liability, guilt, innocence, intent, or wrongdoing. It determines only the classification label, handling constraints, and required safeguards.

4. Scope & Applicability

4.1 **Scope.**
This Policy applies to all Submissions received by the Organisation via Authorised Channels and to all circumstances where any internal personnel, volunteers, systems, or processes interact with Submission content, metadata, or derived materials for any purpose.

4.2 **Applicability.**
This Policy applies to all parties interacting with the Organisation's intake and verification operations, including members of the public, commissioning clients, volunteers, investigators, analysts, contractors, organisational personnel, and automated or semi-automated systems that receive, route, store, or label Submissions.

4.3 **Scope Limitation Clause.**
This Policy governs classification and classification-based constraints only. It does not govern investigative conduct, analytical methodology, archival retention schedules, publication formats, commercial licensing, or any other function outside classification and its immediate handling implications.

5. Definitions (Local Only)

For the purposes of this Policy only:

5.1 **Submission.**
Any material provided to the Organisation for potential consideration, including content and any attached metadata.

5.2 **Source.**
The origin pathway through which a Submission is created, obtained, or conveyed to the Organisation, including the human or system origin, channel of delivery, and provenance attributes.

5.3 **Source Classification.**
A mandatory label assigned under this Policy describing the source type, provenance posture, and reliability handling constraints applicable to a Submission.

5.4 **Provenance.**
Information sufficient to describe how the Submission came into existence and how it came into the submitter's possession, including whether it is direct, copied, derivative, captured, scraped, or third-party relayed.

5.5 **Declared Provenance.**
The provenance statement provided by the submitter (or commissioning entity) at intake.

5.6 **PII.**
Personal Identifiable Information relating to an identified or identifiable natural person.

5.7 **Synthetic Content.**
Content wholly or partially generated, altered, or composed using automated generation, transformation, or simulation techniques, including but not limited to AI-generated text, images, audio, or video.

5.8 **Authorised Channel.**
A controlled intake route designated by the Organisation that supports Assent capture and audit logging.

5.9 **Classification Record.**
The auditable record of the assigned classification label, including timestamp, assignment method, and any reclassification event.

Definitions are local to this Policy and have no binding force outside it.

6. Permitted Activities

Within the strict scope of this Policy, the Organisation may:

6.1 Assign a source classification to each Submission using the taxonomy defined in Section 8.

6.2 Collect and process only the minimum metadata required to determine source classification, including declared provenance and channel identifiers.

6.3 Apply handling constraints, routing rules, and verification prerequisites based on the assigned classification.

6.4 Quarantine or reject Submissions that cannot be classified, are misclassified by the submitter, present unacceptable provenance risk, or trigger prohibitions under Section 7.

6.5 Reclassify a Submission where new provenance facts are obtained, provided that reclassification is auditable and does not retroactively legitimise prior handling.

6.6 Record a Classification Record sufficient to demonstrate procedural compliance.

No other activities are permitted under this Policy.

7. Prohibited Activities

The following are expressly prohibited under this Policy:

7.1 **Unclassified Processing.**
Processing, routing, investigating, analysing, archiving, or publishing any Submission that does not have an assigned source classification under this Policy.

7.2 **Classification Laundering.**
Assigning a classification label intended to upgrade, sanitise, or legitimise a Submission whose declared or apparent provenance does not support that label.

7.3 **Truth Inference from Classification.**
Treating any source classification label as evidence of truth, accuracy, or correctness.

7.4 **Suppression of Provenance Uncertainty.**
Assigning a classification that conceals, minimises, or omits known uncertainties in provenance, including missing chain-of-possession information.

7.5 **Processing of Prohibited Provenance.**
Continuing to process Submissions where declared or apparent provenance indicates coercion, intrusion, unlawful access, extortion, impersonation, or other acquisition methods inconsistent with lawful and ethical handling.

7.6 **Uncontrolled Use of Synthetic Content.**
Treating synthetic content as primary evidence without explicit labelling and heightened containment controls.

7.7 **Reclassification Without Record.**
Reclassifying any Submission without creating a Classification Record.

8. Procedural Requirements

8.1 **Mandatory Classification Sequence.**
Every Submission must undergo the following steps:

a) **Channel Confirmation:** confirm receipt via an Authorised Channel.
b) **Assent Confirmation:** confirm Assent has been recorded.
c) **Declared Provenance Capture:** obtain declared provenance sufficient to classify.
d) **Source-Type Assignment:** assign the appropriate Source Type label from Section 9.
e) **Provenance Posture Assignment:** assign the appropriate Provenance Posture label from Section 9.
f) **Synthetic/Manipulation Flagging:** apply flags where synthetic or altered content is suspected or declared.
g) **Classification Record Creation:** record classification labels, timestamp, and assignment method.
h) **Constraint Application:** apply constraints mandated for that classification under Section 9.
i) **Disposition Routing:** route or reject according to classification constraints.

8.2 **No Deviation.**
No deviation from this sequence is permitted. Any deviation constitutes a breach under Section 11.

8.3 **Classification Is a Gate, Not a Debate.**
Where provenance cannot be sufficiently determined to assign a defensible classification, the Submission must be treated as unclassifiable and must not proceed.

9. Safeguards & Risk Controls

9.1 Source Classification Taxonomy (Mandatory Labels)

Each Submission must receive **two primary labels** and may receive additional flags:

Primary Label A: Source Type (choose exactly one)
A1. **Commissioned Client Material** (provided by a commissioning entity within a formal engagement)
A2. **Public Submission** (provided by a member of the public outside a formal engagement)
A3. **Open-Source Public Record** (derived from publicly accessible official records)
A4. **Open-Source Web Capture** (captured from public web pages, including screenshots/HTML captures)
A5. **Third-Party Report or Publication** (journalism, reports, academic or NGO publications)
A6. **Corporate Disclosure** (annual reports, filings, press releases, published statements)
A7. **User-Generated Content** (forums, social platforms, comment threads, posts)

A8. **Sensor/Telemetry Export** (logs or system exports provided by a party claiming control of the system)
A9. **Unknown/Unverified Origin** (origin not reliably established)

Primary Label B: Provenance Posture (choose exactly one)
B1. **First-Hand** (originator provides the material directly)
B2. **Second-Hand** (submitter relays material from another party)
B3. **Derivative** (summaries, extracts, transformations, paraphrases)
B4. **Captured** (screenshots, recordings, exports)
B5. **Aggregated** (compiled from multiple sources)
B6. **Unclear** (insufficient provenance detail)

Mandatory Flags (apply where relevant; multiple permitted)
F1. **PII Present**
F2. **Special Category Data Present**
F3. **Synthetic/Generated Suspected or Declared**
F4. **Manipulation/Editing Suspected**
F5. **Chain-of-Possession Incomplete**
F6. **Coercion/Extortion Indicator**
F7. **Intrusion/Unauthorised Access Indicator**
F8. **Bad-Faith Pattern Indicator**
F9. **Time-Sensitivity Indicator** (risk of loss, deletion, or imminent harm)

9.2 Default Handling Constraints by Classification

Classification imposes constraints that must be applied immediately:

- **Any Submission with A9 or B6** must be treated as high-risk provenance and must not proceed to investigative or analytical use unless and until provenance is clarified sufficiently to remove A9/B6 status.
- **Any Submission with F7 (Intrusion/Unauthorised Access Indicator)** is presumptively ineligible for progression and must be rejected or quarantined pending legal-risk review.
- **Any Submission with F6 (Coercion/Extortion Indicator)** must be rejected and logged as a prohibited provenance indicator.
- **Any Submission with F3/F4 (Synthetic/Manipulation)** must be labelled as such and must not be treated as primary evidence; it may only be used as a lead indicator subject to heightened verification prerequisites and explicit downstream restrictions.
- **Any Submission with F1/F2 (PII/Special Category)** must be contained with heightened access restrictions; classification must never be used to justify public dissemination.

9.3 Data Minimisation in Classification

Classification must be determined using the minimum necessary provenance and channel information. Classification is not a pretext for collecting additional personal data.

9.4 Misclassification Handling

Where the submitter's declared provenance appears inconsistent, incomplete, or contradictory, the Submission must be labelled with **F5 Chain-of-Possession Incomplete** and/or assigned **A9/B6** as appropriate, and must be blocked from progression until clarified.

9.5 Reclassification Controls

Reclassification is permitted only where new provenance facts are obtained. Reclassification must:
a) create a new Classification Record;
b) preserve prior labels historically (no deletion of history);
c) explicitly state that reclassification does not retroactively legitimise any prior handling.

9.6 Non-Endorsement Safeguard

No classification label implies truth, accuracy, legality, or admissibility in court. It is a procedural label only.

10. Enforcement & Compliance Mechanisms

10.1 **Hard Gating.**
Internal workflows must prevent any Submission from progressing without Source Type and Provenance Posture labels, plus required flags.

10.2 **Audit Logging.**
Classification assignment, flags, and reclassification events must be recorded with timestamps, channel identifiers, and assignment method.

10.3 **Access Controls Based on Flags.**
Submissions labelled with PII/Special Category and/or prohibited provenance indicators must be automatically restricted to the minimum number of authorised roles required to make an eligibility decision.

10.4 **Periodic Internal Checks.**
The Organisation may perform internal checks to detect classification drift, upgrading behaviour, or inconsistent application.

11. Breach Handling & Remediation

11.1 **Breach Definition.**
A breach includes, without limitation:
a) progressing an unclassified Submission;
b) upgrading or laundering a classification label to permit progression;
c) failing to apply required flags;
d) suppressing provenance uncertainty;
e) reclassifying without a Classification Record.

11.2 **Containment.**
On detection or credible allegation of breach, the Organisation will quarantine affected Submissions, suspend progression pathways, and restrict access pending review.

11.3 **Corrective Action Record.**
The Organisation will create an internal breach record documenting detection, containment, corrective action, and closure, retained as an operational defence artefact.

11.4 **Remediation.**
Remediation may include re-performing classification under correct procedure, reversing improper progression, secure deletion of materials processed contrary to constraints, and tightening intake channel controls.

12. Limitation of Liability

12.1 **Scope-Limited Role.**
Within the scope of classification, the Organisation's role is to assign procedural labels and constraints. The Organisation does not warrant that any Submission is accurate, truthful, lawful, complete, or suitable for any purpose.

12.2 **No Liability for Classification Decisions.**
The Organisation is not liable for outcomes arising from classification, refusal to classify, rejection due to provenance risk, or constraints applied under this Policy.

12.3 **No Liability for Submitter Misrepresentation.**
The Organisation is not liable for consequences arising from submitter misrepresentation of provenance, lawful basis, chain-of-possession, or content integrity.

12.4 **No Liability for Reliance Beyond Scope.**
The Organisation is not liable for any reliance by submitters or third parties on classification labels as implying truth, legality, or endorsement.

12.5 **No Exclusion Where Prohibited by Law.**
Nothing in this Policy limits liability to the extent prohibited by applicable law.

13. Non-Delegation & Non-Expansion Clause

13.1 **No Delegation.**
This Policy does not confer investigative, analytical, archival, publication, enforcement, or decision-making authority beyond classification and constraint application.

13.2 **No Expansion.**
This Policy may not be interpreted to authorise activities outside its defined scope or to override other organisational controls.

13.3 **No Legal Determination.**
Classification is a procedural risk control and does not constitute a determination of legality, wrongdoing, or liability as a matter of law.

14. Jurisdiction & Governing Law

14.1 **Governing Law.**
This Policy is governed by the laws of **England and Wales**.

14.2 **Forum.**
Subject to mandatory statutory requirements that cannot be excluded, disputes arising from or materially connected to this Policy fall within the jurisdiction of the courts of **England and Wales**.

14.3 **Mandatory Compliance Carve-Out.**
Nothing in this section is intended to disapply mandatory statutory obligations that apply based on the location of processing, data subjects, or other non-excludable legal requirements.

15. Amendments & Version Control

15.1 **Amendment Right.**
This Policy may be amended solely by the Organisation.

15.2 **Publication and Effect.**
Amendments take effect upon publication of an updated version number and effective date.

15.3 **Acceptance of Updates.**
Continued engagement, commissioning, submission, or use of intake channels after publication of an amended version constitutes acceptance of the amended Policy.

15.4 **Version Evidence.**
The Organisation will retain the version identifier associated with recorded Assent and the Classification Record.

16. Supremacy Within Scope

16.1 **Authoritative Within Scope.**
Within the domain of source classification and classification-based constraints, this Policy is authoritative.

16.2 **No Force Outside Scope.**
Outside the domain defined in Section 4, this Policy has no force and may not be construed to govern other organisational functions.