OFFICIAL STANDARDS DOCUMENT

Version 1.0 · April 2026 · sobir.ca

SOCIETY FOR ORIGINAL BIOMETRIC IDENTITY RIGHTS · BC SOCIETY S0083123

SOBIR Entity Assessment Standards Framework

Criteria for the Assessment of Any Entity Operating in the Biometric Identity Space

This document establishes the five criteria against which SOBIR assesses any entity whose design, operation, or deployment involves the collection, processing, generation, distribution, storage, or replication of human biometric identity data. Certification under this framework is earned through assessment and is subject to ongoing review. Payment of any fee does not guarantee certification.

ISSUING BODY

Society for Original Biometric Identity Rights
BC Society No. S0083123

VERSION

1.0 — April 2026
Annual review cycle

WEBSITE

sobir.ca

PREAMBLE

Context and Rationale

The proliferation of AI systems capable of replicating human voice, generating synthetic likeness, and processing biometric identity data at scale has produced a category of harm that existing standards frameworks were not designed to address. The capacity to reproduce who a person is — their voice, their face, their physiological identity — now outpaces the governance mechanisms intended to protect them.

This is not a future concern. It is a present condition. Voice cloning is used in financial fraud. Synthetic likeness is deployed without consent. Biometric data collected by entities on the promise of protection is vulnerable to misuse by those same entities, by their investors, and by external actors who compromise their systems. The individuals whose data this is bear the consequences.

The Society for Original Biometric Identity Rights was established to address this gap directly. SOBIR is a registered BC Society (S0083123) operating as an independent standards and advocacy body. The framework is designed to remain applicable as the technology continues to evolve.

DEVELOPMENT

Basis of Assessment Authority

SOBIR's assessment authority derives from its mandate as a registered standards and advocacy body established specifically to address the governance gap in biometric identity protection. The criteria in this framework were developed through sustained engagement with the technical, legal, and lived dimensions of biometric identity harm — including direct experience as a working professional whose voice and likeness were subject to unauthorized AI replication, published framework work in the field of AI ethics, and ongoing engagement with academic researchers, legal practitioners, and policy contacts working on AI identity governance.

SOBIR draws on independent expertise appropriate to the entity type under assessment. Where assessment requires technical, legal, or domain-specific knowledge beyond SOBIR's primary expertise, SOBIR engages qualified independent reviewers. All assessors are subject to SOBIR's conflict of interest policy. SOBIR's criteria development and review process is documented and available upon request.

SCOPE OF APPLICATION

Definition of Entity

The following definition governs the scope of this framework. All subsequent references to entity in this document carry this meaning.

FORMAL DEFINITION

For the purposes of this framework, entity refers to any organization, company, developer, operator, or autonomous system — regardless of size, jurisdiction, or commercial status — whose design, operation, or deployment involves the collection, processing, generation, distribution, storage, or replication of human biometric identity data, whether directly or as a component of a broader system. This includes entities that act on behalf of humans, entities that operate without continuous human oversight, and entities

whose outputs may be used by others to engage with human biometric identity data. The obligations of this framework attach to the point of contact with biometric identity data, not to organizational form.

MULTI-ENTITY AND AGENTIC SYSTEMS

Where multiple entities in a pipeline collectively process biometric identity data, each entity is assessed against the criteria applicable to its specific point of contact. Where accountability for a given processing activity is disputed between entities in a pipeline, SOBIR will assess the entity with the greatest operational control over the relevant processing activity as the responsible entity, unless the entities jointly submit a documented accountability allocation that SOBIR accepts as part of the scoping process.

DATA TYPES IN SCOPE

Voice and audio biometrics · Facial likeness and visual identity · Physiological and behavioral identifiers · Any data from which an individual's identity may be inferred, replicated, or reconstructed by technical means

ASSESSMENT COVERAGE

Assessment is conducted against all five criteria regardless of entity type. Criteria weighting may be adjusted to reflect an entity's specific operational profile as determined by SOBIR during the scoping process.

On Certification: SOBIR certification is not a product and cannot be purchased. It is a formal recognition that an entity has met the standards contained in this framework at the time of assessment, as determined solely by SOBIR. Certification may be granted, withheld, suspended, or revoked. The submission of an assessment application and the payment of any associated fee confer no rights to the SOBIR verification mark and do not constitute or imply a commitment to certify.

ASSESSMENT CRITERIA

SOBIR Assessment Standards

Assessment against all five criteria is required for SOBIR certification. No criterion may be waived, substituted, or deferred. Normative requirements within each criterion are mandatory conditions of conformance. Instructive requirements provide additional guidance on implementation but are not themselves conditions of certification.

CRITERION I

Consent and Authorization

PRINCIPLE

The right of every individual to determine how their voice, likeness, and biometric identity is collected, used, and distributed is absolute. No biometric identifier may be processed, replicated, or transmitted without the free, informed, specific, and documented consent of the originating individual. Consent is personal, non-transferable, and revocable at any time without penalty. Authorization obtained through ambiguous, buried, or coercive terms does not constitute consent under SOBIR standards.

DEFINITION — DARK PATTERNS

For the purposes of this criterion, dark patterns refers to interface design choices that manipulate or deceive users into actions they would not take if they fully understood what they were doing. This includes but is not limited to: confirmshaming, hidden defaults, obstruction, forced continuity, misdirection, and interface friction specifically applied to consent withdrawal or decline pathways. SOBIR applies the definition established in the EU Digital Services Act Article 25 and the established academic taxonomy of deceptive design patterns as reference points in assessment.

NORMATIVE REQUIREMENTS

CONSENT ARCHITECTURE

- Consent must be architecturally coupled to data processing — the technical system must be designed such that withdrawal of consent has a direct effect on data processing, not merely on a consent record
- Consent for biometric data must be granular and sequential — consent to collect, consent to process, consent to use in model training, and consent to share with third parties are distinct acts, each independently revocable
- Consent interfaces must be designed such that withholding or withdrawing consent does not degrade the core functionality of the service — consent must not be a condition of access. This requirement applies to the entire consent lifecycle. Dark patterns applied at any stage — including friction introduced to the withdrawal process, confirmation dialogs designed to discourage withdrawal, and re-consent prompts that obscure the option to decline — are violations of this criterion regardless of whether the initial consent interface was compliant

DATA AND MODEL OBLIGATIONS

- Consent withdrawal must trigger verifiable deletion or deactivation of biometric data within a defined and disclosed timeframe, including from derived data products, model embeddings, and third-party copies. Where complete deletion of derived data is not technically achievable, the entity must document why, disclose this limitation to the individual at the point of consent, and implement the nearest available alternative that minimises residual data exposure
- Where biometric data has been used in model training, the entity must disclose this use explicitly at the point of consent. Upon consent withdrawal, the entity must either implement a documented technical remediation pathway — including model unlearning, retraining without the individual's data, or equivalent mechanism — with a defined completion timeline disclosed to the individual, or, where no such pathway is currently available, provide the individual with written disclosure of that limitation at the point of consent, including what residual data exposure remains and what steps the entity commits to taking as remediation capability develops. A documented position that remediation is not feasible, without disclosure to the individual and a committed improvement timeline, does not satisfy this requirement. For the purposes of this requirement, an equivalent mechanism is one that demonstrably reduces the influence of the individual's biometric data on model outputs to a level that SOBIR determines is materially equivalent to deletion, based on documented technical evidence submitted by the entity
- Biometric data terms must be presented as a standalone disclosure, separate from general terms of service, prior to any collection activity
- Entities may not submit repeated re-consent requests to individuals who have previously withdrawn consent for a specific processing activity. A minimum interval between re-consent requests must be defined and disclosed, and re-consent requests must be presented with equal visual prominence to the decline option

CRITERION II

Disclosure and Transparency

PRINCIPLE

Individuals interacting with any system that collects, processes, or generates biometric identity data have an unconditional right to know. Entities must proactively disclose when AI-generated, AI-altered, or AI-processed content or identity data is involved, including the nature of that involvement, its purpose, and its limitations. Disclosure must be accessible without the user seeking it out. Obscuring the synthetic or processed nature of content or data — whether through interface design, labeling omissions, or contractual terms — constitutes a violation of identity trust under SOBIR standards.

NORMATIVE REQUIREMENTS

- Clear, visible labeling of AI-generated or AI-altered content involving human identity at the point of interaction, not only in documentation

- Proactive disclosure of data processing activities affecting biometric identity, including retention periods, third-party access, and model training use, prior to collection
- Where synthetic biometric content is generated or distributed, entities must implement technical mechanisms for provenance attribution that enable the origin and synthetic nature of that content to be verified by independent parties. Provenance mechanisms must be designed to resist removal, manipulation, or spoofing — a provenance signal that can be stripped without detection does not satisfy this requirement. Entities must demonstrate robustness through periodic independent testing of provenance mechanisms against known removal and manipulation methods, conducted at intervals defined during the scoping process and documented in the assessment record
- Documentation of system limitations relevant to identity accuracy, replication fidelity, and detection capability, made accessible to users and affected parties
- Interface design must not obscure the distinction between original and synthetic identity through visual, auditory, or contextual framing

CRITERION III

Harm Prevention and Misuse Controls

PRINCIPLE

> Human biometric identity may not be weaponized. Entities operating in the biometric identity space bear active responsibility for preventing their systems from being used to impersonate, defraud, harass, exploit, or cause reputational, financial, or personal harm to individuals through their voice, likeness, or identity data. Passive prohibition through terms of service is not sufficient. Entities bear an ongoing operational responsibility to anticipate foreseeable misuse, implement technical and policy controls commensurate with the risk profile of their systems, and demonstrate that those controls are active and maintained.

NORMATIVE REQUIREMENTS

RISK ASSESSMENT

- Documented misuse risk assessment specific to the entity's biometric identity functions, conducted prior to deployment and reviewed on a defined cycle
- Risk assessment must identify the highest-probability misuse vectors including impersonation, fraud, non-consensual synthetic media, and coordinated identity deception

ACTIVE CONTROLS

- Technical controls addressing each high-probability misuse vector identified in the risk assessment, with evidence of implementation and ongoing operation
- Policy controls that assign organizational accountability for misuse prevention, distinct from general terms of service prohibitions
- Evidence of active monitoring for misuse patterns rather than reactive response only, with defined escalation and response protocols
- Controls must be reviewed and updated following any identified misuse incident

CRITERION IV · PRIMARY STANDARD

Biometric Data Fiduciary Responsibility

PRINCIPLE

> Any entity that collects or holds biometric identity data assumes a fiduciary duty to the individuals whose identity that data represents. (SOBIR uses the term fiduciary in the sense of trusted stewardship — a duty of care owed to the individuals whose irreplaceable identity data is held. This is a standards obligation, not a legal designation, and does not create fiduciary duties in the specific legal sense that varies by jurisdiction. Assessed entities and their legal counsel should seek independent legal advice on the jurisdictional implications of their data governance obligations.) This duty supersedes commercial interest, investor pressure, and operational convenience. It exists because biometric data is irreplaceable — unlike a password or an account number, a voice or a face cannot be reissued if compromised. Entities must demonstrate documented governance structures that reflect this duty in practice, not only in policy. Biometric data held in trust must never become a commodity.

NORMATIVE REQUIREMENTS

GOVERNANCE STRUCTURE

- Documented data governance policies specific to biometric identity data, separate from general privacy policies
- Documented access controls with explicit limitations on third-party access, investor access, and use of biometric data for purposes beyond the stated collection purpose
- Evidence that data minimization principles are applied — only biometric data necessary for the stated function is collected and retained

INTERNAL ACCESS CONTROLS

- Documented role-based access controls limiting internal access to biometric data to personnel with defined operational need
- Audit logging capturing all internal access events involving biometric data, including access by administrators, engineers, and contractors, retained for a defined period and accessible for review in the event of a suspected insider incident
- Access privileges reviewed on a defined cycle and revoked immediately upon change of role or departure

BREACH AND DELETION

- Breach notification protocols with defined timelines and individual notification obligations specific to biometric data incidents
- Unqualified right of deletion exercisable by the individual without legal prerequisite, technical barriers, or service degradation
- Documentation of what deletion means technically — including derived data, model weights trained on the individual's data, and third-party copies

INVESTOR AND COMMERCIAL PROTECTIONS

- Documented policies governing what happens to biometric data in the event of acquisition, merger, investor pressure, or insolvency
- Evidence that biometric data is classified as a protected asset within the entity's governance structure, not a commercial asset, and that its transfer, sale, or repurposing is prohibited under the entity's own policies. Entities must maintain a documented biometric data protection plan that activates in the event of acquisition, merger, change of control, or insolvency proceedings. This plan must include: notification obligations to affected individuals, deletion protocols that take effect prior to any asset transfer where legally permissible, and designated accountability for executing the plan. SOBIR acknowledges that court-ordered transfers in insolvency proceedings may override contractual protections. The requirement here is not to override law but to demonstrate that the entity has taken every available step within legal limits to protect biometric data before any such transfer occurs

On Criterion IV: Biometric Data Fiduciary Responsibility is the primary standard of the SOBIR framework. It reflects the recognition that entities collecting biometric identity data on the promise of protecting it are subject to commercial, investor, and operational pressures that can directly conflict with that promise. The tension between fiduciary duty and commercial incentive is the central governance challenge of the biometric identity space. SOBIR's assessment of this criterion is the most substantive component of the review process.

CRITERION V

Accountability and Remediation

PRINCIPLE

> Acknowledgment of potential harm is not accountability. Policy statements are not accountability. Accountability in the biometric identity context requires documented, operational protocols for responding to violations, breaches, and misuse — and clear remediation pathways accessible to the individuals whose biometric identity has been compromised. The burden of navigating those pathways must not fall on the affected individual. Entities bear the responsibility of making remediation accessible, timely, and proportionate to the harm caused.

NORMATIVE REQUIREMENTS

- Documented incident response protocols covering biometric identity breaches and misuse, with defined timelines for each stage of response
- Defined remediation pathways accessible to affected individuals without legal prerequisite, financial cost to the individual, or requirement to prove harm before accessing the pathway
- Evidence that affected individuals are notified of incidents that implicate their biometric data within a defined and disclosed timeframe
- Designated accountability function within the entity with documented authority to activate remediation protocols
- Post-incident review mechanisms that assess the adequacy of remediation and result in documented improvements to prevent recurrence

RECIPROCAL OBLIGATIONS

SOBIR's Obligations to Assessed Entities

Assessment is a bilateral process. SOBIR holds assessed entities to rigorous standards. Assessed entities are entitled to expect equivalent standards from SOBIR in the conduct of assessment. The following obligations are binding on SOBIR in all assessment engagements.

CONFIDENTIALITY

All documentation submitted by an assessed entity in the course of assessment is treated as confidential. SOBIR will not disclose, publish, or reference submitted documentation without the written consent of the assessed entity, except where disclosure is required by law. SOBIR commits to retaining submitted documentation only for the period necessary to conduct and record the assessment, and to providing assessed entities with a written statement of how their documentation was handled upon completion of the assessment process. Assessed entities may request confirmation of documentation disposal at any time.

CONFLICTS OF INTEREST

SOBIR will not conduct an assessment where a material conflict of interest exists. Any actual or potential conflict identified prior to or during assessment must be disclosed to the assessed entity. The assessed entity may request reassignment of the assessment on grounds of conflict without prejudice to their application.

TRANSPARENT DECISIONS

All assessment decisions — whether to certify, withhold, suspend, or revoke — will be accompanied by a written findings document that states the basis for the decision with reference to specific criteria and normative requirements. SOBIR will not issue decisions without written justification.

APPEALS PROCESS

An assessed entity that receives an adverse decision may submit a formal written appeal within 30 days of receiving the decision. Appeals are reviewed independently of the original assessor. SOBIR will issue a written acknowledgment of receipt within 20 business days. A substantive written response addressing the grounds of the appeal will be issued within 60 days of receipt of the

acknowledgment. The substantive response will either uphold the original decision with written justification, reverse the original decision with written justification, or, in exceptional circumstances, extend the review period by a further 30 days with written explanation. A substantive response constitutes SOBIR's final decision on the appeal unless new material evidence is submitted.

CONSISTENT APPLICATION

SOBIR applies the criteria in this framework consistently across all assessed entities regardless of size, commercial status, or relationship to SOBIR. No entity receives preferential treatment in the assessment process.

FRAMEWORK CURRENCY

SOBIR commits to reviewing this framework on an annual basis. Assessed entities will be notified of material changes to criteria or normative requirements before those changes take effect for certification renewal purposes.

PROCESS

Assessment Process

1

ENQUIRY AND SCOPING

SOBIR reviews the applying entity's operational profile and determines applicable criteria weighting, required evidence categories, timeline, and fee structure. Submission of an enquiry does not initiate assessment and does not constitute a commitment by SOBIR to assess.

2

DOCUMENTATION SUBMISSION

The applying entity submits documentation against each criterion as specified by SOBIR following the scoping process. Required evidence is defined based on the entity's operational profile. Incomplete submissions will not proceed to review.

3

ASSESSMENT REVIEW

SOBIR conducts a structured review against each criterion and its normative requirements. Assessment draws on SOBIR's published standards framework, biometric identity rights research, and expertise encompassing the technical, legal, and industry dimensions of biometric identity harm.

4

WRITTEN DECISION

SOBIR issues a formal written decision with findings referenced to specific criteria and normative requirements. Where all normative requirements are met, the SOBIR verification mark is licensed for display. Where requirements are not met, a detailed findings document is issued.

5

ANNUAL REVIEW

Certified entities are subject to annual review. Certification may be renewed, suspended, or revoked based on changes to the entity's practices, policies, or conformance with SOBIR standards at the time of review.

VERSIONING

Framework Versioning

The biometric identity space is evolving rapidly. This framework is designed to remain applicable as technology develops, but the normative requirements within each criterion will be reviewed and updated to reflect material changes in the risk landscape, available technical standards, and regulatory developments.

ANNUAL REVIEW PROCESS

SOBIR conducts a formal review of this framework each April. The review assesses whether criteria remain current, whether normative requirements reflect the technical state of the field, and whether new entity types or data types require scope adjustment. Review findings are published at sobir.ca.

VERSION CHANGE PROTOCOL

Minor updates — clarifications, additions to normative requirements — are versioned as point releases (e.g. V1.1). Material changes to criteria or scope are versioned as major releases (e.g. V2.0). Certified entities are notified of any version change before it takes effect for renewal purposes, with a minimum 90-day notice period for major releases.