SOCIETY FOR ORIGINAL BIOMETRIC IDENTITY RIGHTS · BC SOCIETY S0083123

A Framework of Practice for the Use of Biometric Identity

This document proposes five criteria of practice for any entity whose design, operation, or deployment involves the collection, processing, generation, distribution, storage, or replication of biometric data. It is published by the Society for Original Biometric Identity Rights (SOBIR), alongside *A Standard of Consent for the Use of Biometric Identity* (the "Standard"), as a proposal for voluntary adoption by organizations, independent assessors and policymakers. SOBIR does not assess or certify any entity.

ISSUING BODY
Society for Original Biometric Identity Rights

VERSION
2.0 — November 2026

© 2026 Society for Original Biometric Identity Rights. All rights reserved.

SOCIETY FOR ORIGINAL BIOMETRIC IDENTITY RIGHTS

DOCUMENT STATUS

Published

NEXT SCHEDULED REVIEW

April 2027

SUPERSEDES

SOBIR Entity Assessment Standards Framework, Version 1.1 (October 2026). Version 2.0 renames and repositions this framework as criteria of practice supporting the Standard, removes provisions for assessment and certification by SOBIR, aligns definitions and Criterion 1 with the Standard, and generalizes the assessment process and assessor obligations for use by independent assessors and authorities.

STATUS

SOBIR publishes this framework as a proposal for voluntary adoption. SOBIR does not assess or certify any entity. Any organization may apply these criteria to its own practices, and independent assessors and authorities may use them. Where this framework and the Standard differ, the Standard prevails. Correspondence: admin@sobir.ca

INTELLECTUAL PROPERTY NOTICE

This document is the intellectual property of the Society for Original Biometric Identity Rights. All rights reserved. This document may be referenced and cited with full attribution to SOBIR, Version 2.0, November 2026. It may not be reproduced in whole or in part, adapted, repackaged, or represented as the work of any other organization without the express written permission of SOBIR, except as permitted by law, including fair dealing. Unauthorized reproduction of this document — including reproduction for commercial purposes — constitutes infringement of SOBIR's intellectual property rights.

CONTENTS

Table of Contents

Inside Cover & IP Notice 2

Introduction 4

Clause 1 — Scope 5

Clause 2 — Normative References 6

Clause 3 — Terms and Definitions 6

Clause 4 — Criterion 1: Consent and Authorization 8

Clause 5 — Criterion 2: Disclosure and Transparency 10

Clause 6 — Criterion 3: Harm Prevention and Misuse Controls 11

Clause 7 — Criterion 4: Biometric Data Fiduciary Responsibility 12

Clause 8 — Criterion 5: Accountability and Remediation 14

Clause 9 — Application and Assessment 15

Annex A (normative) — Obligations of Assessors 16

Annex B (informative) — Forward Compatibility Statement 18

INTRODUCTION

Introduction

0.1 Background. The emergence of AI systems capable of replicating, generating, and processing biometric data at scale — including voice, facial likeness, and physiological identifiers — has created a category of risk that existing standards frameworks do not comprehensively address. The technical capacity to reproduce identifiable human characteristics now exceeds the governance mechanisms available to individuals and institutions seeking to manage the associated harms.

This framework was developed in response to that gap. The Society for Original Biometric Identity Rights (SOBIR) is a registered BC society (No. S0083123) that develops and proposes standards, and advocates for the protection of biometric identity. The framework is designed to remain applicable as the relevant technology continues to develop.

0.2 Relationship to Other Standards. This framework draws on the structural conventions of ISO/IEC conformity assessment standards, in particular ISO/IEC 17021-1, which informs the procedural architecture of the assessment process in Clause 9 and the assessor obligations in Annex A. The EU Digital Services Act Article 25 and established academic taxonomies of deceptive design patterns are referenced as definitional baselines within the criteria.

This framework is an independent standard. It is not affiliated with, endorsed by, or derived from ISO, IEC, or the institutions responsible for the instruments referenced above. Reference to those instruments does not imply that assessed entities are legally subject to them.

0.3 Purpose of Publication. SOBIR publishes this framework so that its criteria can inform practice, procurement, assessment, research and policy. Any organization may apply the criteria to its own systems, independent assessors and authorities may use them, and any person or institution may cite them with attribution. SOBIR does not assess or certify any entity.

0.4 Relationship to the Standard. *A Standard of Consent for the Use of Biometric Identity* (the “Standard”) sets out the rights of persons and the obligations of developers, commissioning parties and platforms regarding consent to the use of biometric data. This framework sets out the criteria of practice by which an entity can meet those obligations and govern biometric data responsibly. Terms defined in the Standard have the same meaning in this framework. Where this framework and the Standard differ, the Standard prevails.

CLAUSE 1

Scope

This document applies to any entity whose design, operation, or deployment involves the collection, processing, generation, distribution, storage, or replication of biometric data, whether directly or as a component of a broader system. This document applies regardless of the entity's size, jurisdiction, or commercial status. The obligations of this framework attach to the point of contact with biometric data, not to organizational form.

This document applies to the following categories of data: voice and audio biometrics; facial likeness and visual identity; physiological and behavioural identifiers; and any data from which an individual's identity may be inferred, replicated, or reconstructed by technical means.

Nothing in this framework requires an entity to act contrary to applicable law. Where law requires the processing of biometric data without consent, the entity shall document the legal basis and limit processing to what the law requires.

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 the assessor during scoping.

CLAUSE 2

Normative References

— **ISO/IEC 17021-1:2015** — Conformity assessment. Referenced for structural and procedural conventions applied to the assessment process (Clause 9) and assessor obligations (Annex A).

— **EU Digital Services Act, Article 25** (Regulation (EU) 2022/2065) — Prohibition on dark patterns. Referenced as definitional baseline for dark patterns within Criterion 1.

— **Gray et al. (2018)** — "The Dark (Patterns) Side of UX Design." CHI 2018. ACM. Referenced in Criterion 1 as supplementary definitional resource for consent interface design assessment.

— **Content Credentials: C2PA Technical Specification** (latest version) — Technical standard for content provenance and authenticity attribution. Referenced in Criterion 2 as a recognized technical mechanism for provenance attribution.

— **ISO/IEC 27001:2022** — Information security management systems. Referenced in Criterion 4 as a baseline standard against which biometric data governance structures may be benchmarked. Certification to ISO 27001 does not constitute satisfactory evidence of conformance with Criterion 4 in isolation.

CLAUSE 3

Terms and Definitions

Within normative text: **shall** indicates a requirement strictly to be followed with no deviation permitted; **should** indicates a recommendation that is preferred but not strictly required; **may** indicates a permissible course of action.

3.1 ENTITY

Any individual acting in the course of a business, profession or other paid or public-facing activity, and 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 biometric data, whether directly or as a component of a broader system. The obligations of this framework attach to the point of contact with biometric data, not to organizational form. Where multiple entities in a pipeline collectively process biometric data, each is assessed against the criteria applicable to its specific point of contact. Where the entity is an autonomous system, the obligations of this framework attach to the individual or organization that deploys or operates it.

3.2 BIOMETRIC DATA AND DIGITAL REPLICA

As defined in the Standard. Biometric data includes recordings, images, scans and measurements of a person's voice, face, body or movement, at any age or stage of life, and any feature, embedding, model or output derived from them. A digital replica is a computer-generated or computer-altered representation of a person that is readily identifiable as that person.

3.3 DARK PATTERNS

Interface design choices that manipulate or deceive users into actions they would not take if fully informed. Includes confirmshaming, hidden defaults, obstruction, forced continuity, misdirection, and friction applied to consent withdrawal. Reference: EU DSA Article 25 and Gray et al. (2018).

3.4 REQUIREMENT TIERS

Primary (Criteria 1 and 4): failure of any shall requirement is a major non-conformity.
Essential (Criteria 3 and 5): failure is a conditional finding, pending remediation.
Operational (Criterion 2): shall provisions mandatory; should provisions may be accepted with documented improvement commitments.

3.5 FIDUCIARY DUTY

As used in this framework: a duty of trusted stewardship owed to individuals whose biometric data an entity holds. 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 should seek independent legal advice on jurisdictional implications.

3.6 ASSESSOR

Any person or body applying this framework to assess an entity, including the entity itself, an independent assessor or an authority designated under applicable law.

CLAUSE 4 · CRITERION 1

PRIMARY REQUIREMENT

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 as against any commercial or contractual interest. No biometric identifier shall be processed, replicated, or transmitted without the free, informed, specific, and documented consent of the originating individual. Consent is personal and non-transferable, and may be withdrawn in accordance with the Standard; a valid licence binds both parties for its stated duration and within its stated terms. Authorization obtained through ambiguous, buried, or coercive terms does not constitute consent under SOBIR standards.

NORMATIVE REQUIREMENTS

CONSENT ARCHITECTURE

— Consent shall be architecturally coupled to data processing — the technical system shall be designed such that withdrawal of consent has a direct effect on data processing, not merely on a consent record

— Consent for biometric data shall 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 shall be designed such that withholding or withdrawing consent does not degrade core service functionality — consent shall not be a condition of access. This requirement applies to the entire consent lifecycle. Dark patterns (defined in 3.3) applied at any stage — including friction on withdrawal, confirmation dialogs designed to discourage withdrawal, and re-consent prompts that obscure the decline option — are violations of this clause regardless of whether the initial consent interface was compliant

DATA AND MODEL OBLIGATIONS

— Consent withdrawal, where permitted under the Standard, shall 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, except works completed under a valid licence, which may continue to be used within its terms. Where complete deletion is not technically achievable, the entity shall document why, disclose this limitation at the point of consent, and implement the nearest available alternative that minimizes residual data exposure

- Where biometric data has been used in model training, the entity shall disclose this use explicitly at the point of consent. Upon withdrawal, the entity shall 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 provide written disclosure of that limitation with a committed improvement timeline. A documented position that remediation is not feasible, without disclosure and a committed timeline, does not satisfy this requirement
- Biometric data terms shall be presented as a standalone disclosure, separate from general terms of service, prior to any collection activity
- Entities shall 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 shall be defined and disclosed, and re-consent requests shall be presented with equal visual prominence to the decline option

CLAUSE 5 · CRITERION 2

OPERATIONAL REQUIREMENT

Disclosure and Transparency

PRINCIPLE

> Individuals interacting with any system that collects, processes, or generates biometric data have an unconditional right to know. Entities shall 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 shall be accessible without requiring the user to seek it out. Obscuring the synthetic or processed nature of content or data constitutes a violation of identity trust under SOBIR standards.

NORMATIVE REQUIREMENTS

MANDATORY PROVISIONS (SHALL)

— Clear, visible labelling of AI-generated or AI-altered content involving human identity shall be provided at the point of interaction, not only in documentation

— Entities shall proactively disclose 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 shall implement technical mechanisms for provenance attribution that enable the origin and synthetic nature of that content to be verified by independent parties. Provenance mechanisms shall be designed to resist removal, manipulation, or spoofing — a provenance signal that can be stripped without detection does not satisfy this requirement

— Entities shall demonstrate robustness of provenance mechanisms through periodic independent testing against known removal and manipulation methods, conducted at intervals defined during the scoping process and documented in the assessment record

— Interface design shall not obscure the distinction between original and synthetic identity through visual, auditory, or contextual framing

RECOMMENDED PRACTICE (SHOULD)

— Documentation of system limitations relevant to identity accuracy, replication fidelity, and detection capability should be made accessible to users and affected parties

CLAUSE 6 · CRITERION 3

ESSENTIAL REQUIREMENT

Harm Prevention and Misuse Controls

PRINCIPLE

> Human biometric identity shall 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 shall be conducted prior to deployment and reviewed on a defined cycle
- Risk assessment shall identify the highest-probability misuse vectors including but not limited to 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 shall be implemented with evidence of ongoing operation
- Policy controls shall assign organizational accountability for misuse prevention, distinct from general terms of service prohibitions
- Entities shall maintain evidence of active monitoring for misuse patterns with defined escalation and response protocols
- Controls shall be reviewed and updated following any identified misuse incident

CLAUSE 7 · CRITERION 4

PRIMARY REQUIREMENT

Biometric Data Fiduciary Responsibility

PRINCIPLE

> Any entity that collects or holds biometric data assumes a fiduciary duty to the individuals whose identity that data represents. 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 shall demonstrate documented governance structures that reflect this duty in practice, not only in policy. Biometric data held in trust shall never become a commodity.

> **NOTE ON TERMINOLOGY — FIDUCIARY DUTY**
>
> 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.

NORMATIVE REQUIREMENTS

GOVERNANCE STRUCTURE

— Documented data governance policies specific to biometric data, separate from general privacy policies, shall be maintained

— Documented access controls with explicit limitations on third-party access, investor access, and use of biometric data beyond the stated collection purpose shall be maintained

— Evidence shall be provided 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 shall limit internal access to biometric data to personnel with defined operational need

— Audit logging shall capture 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 shall be 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 shall be maintained

— The unqualified right of deletion shall be exercisable by the individual without legal prerequisite, technical barriers, or service degradation, including documentation of what deletion means technically — derived data, model weights, and third-party copies

INVESTOR AND COMMERCIAL PROTECTIONS

— Biometric data shall be classified as a protected asset within the entity's governance structure, not a commercial asset. Its transfer, sale, or repurposing shall be prohibited under the entity's own policies

— Entities shall maintain a documented biometric data protection plan activating in the event of acquisition, merger, change of control, or insolvency. This plan shall include: notification obligations to affected individuals, deletion protocols taking effect prior to any asset transfer where legally permissible, and designated accountability for executing the plan. SOBIR acknowledges that court-ordered transfers in insolvency may override contractual protections. The requirement is to demonstrate every available step within legal limits has been taken

On Criterion 4: Biometric Data Fiduciary Responsibility is the primary criterion of this framework. Failure to satisfy any shall requirement in this clause is a major non-conformity. Assessment of this clause is the most substantive component of any review.

CLAUSE 8 · CRITERION 5

ESSENTIAL REQUIREMENT

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 shall not fall on the affected individual. Entities bear the responsibility of making remediation accessible, timely, and proportionate to the harm caused.

NORMATIVE REQUIREMENTS

INCIDENT RESPONSE

— Documented incident response protocols covering biometric identity breaches and misuse shall be maintained, with defined timelines for each stage of response

— Affected individuals shall be notified of incidents implicating their biometric data within a defined and disclosed timeframe

— A channel shall be maintained through which any person may report a weakness in the entity's safeguards, including any means of removing provenance marking or bypassing a generation block, and reports shall be assessed and addressed within a defined and disclosed timeframe

— Post-incident review mechanisms shall assess the adequacy of remediation and result in documented improvements to prevent recurrence

INDIVIDUAL REMEDIATION

— Defined remediation pathways shall be accessible to affected individuals without legal prerequisite, financial cost, or requirement to prove harm before accessing the pathway

— A designated accountability function shall exist within the entity with documented authority to activate remediation protocols

CLAUSE 9

Application and Assessment

This framework may be applied by an entity to its own practices or by an independent assessor or authority, including in response to a complaint by a person concerned or a member of the public, or under procedures established by applicable law. SOBIR does not conduct assessments. Where an assessment is conducted, the following process should be followed.

1

9.1 SCOPING

The assessor reviews the entity's operational profile and determines applicable criteria weighting, required evidence categories and timeline.

2

9.2 DOCUMENTATION

The entity shall provide documentation against each criterion as specified following scoping. Required evidence is defined based on the entity's operational profile. Incomplete documentation shall not proceed to review.

3

9.3 REVIEW

The assessor conducts a structured review against each criterion and its normative requirements, drawing on technical, legal and industry expertise relevant to biometric identity harm. The assessor is subject to the obligations in Annex A.

4

9.4 WRITTEN FINDINGS

The assessor issues written findings referenced to specific clauses and normative requirements. Outcomes follow the tier classification in Clause 3.4: Primary failures are major non-conformities; Essential failures and Operational failures on shall provisions are conditional findings pending remediation.

5

9.5 PERIODIC REVIEW

An assessed entity should be reviewed at least annually and following any material change to its practices or to this framework.

6

9.6 CONCERNS

Concerns about an entity's practices should be directed to the entity, to an independent assessor or to the competent authority. SOBIR may publish independent research or public commentary based on publicly available information, clearly framed as research rather than assessment findings. Correspondence may be sent through the contact form at sobir.ca or to admin@sobir.ca.

ANNEX A — NORMATIVE

Obligations of Assessors

Assessment is a bilateral process. The following obligations bind any independent assessor or authority applying this framework, and form part of its normative requirements.

A.1 CONFIDENTIALITY

All documentation submitted shall be treated as confidential. The assessor shall not disclose, publish, or reference submitted documentation without the written consent of the assessed entity, except where required by law. The assessor shall retain submitted documentation only for the period necessary to conduct and record the assessment, and shall provide a written statement of how documentation was handled upon completion. Assessed entities may request confirmation of disposal at any time.

A.2 CONFLICTS OF INTEREST

The assessor shall not conduct an assessment where a material conflict of interest exists. Any actual or potential conflict shall be disclosed to the assessed entity. The assessed entity may request reassignment without prejudice.

A.3 TRANSPARENT DECISIONS

All assessment findings shall be accompanied by a written findings document stating the basis for the findings with reference to specific clauses and normative requirements. The assessor shall not issue findings without written justification.

A.4 APPEALS PROCESS

An assessed entity may submit a formal written appeal within 30 days of receiving adverse findings. The assessor shall issue written acknowledgment within 10 business days. A substantive written response shall be issued within 60 days of acknowledgment, either upholding the findings, reversing them, or extending review by 30 days with written explanation. A substantive response constitutes the assessor's final decision unless new material evidence is submitted.

A.5 CONSISTENT APPLICATION

The assessor shall apply criteria consistently across all assessed entities regardless of size, commercial status, or relationship to the assessor. No entity receives preferential treatment in the assessment process.

A.6 FRAMEWORK CURRENCY

SOBIR reviews this framework annually each April. The assessor shall apply the version of this framework in force at the start of an assessment, unless the assessed entity agrees otherwise.

ANNEX B — INFORMATIVE

Forward Compatibility Statement

This annex is informative and does not carry the weight of the normative criteria in Criteria 1 through 5. It identifies areas where assessment methodology is under active development, acknowledged in the interest of transparency.

B.1 ANNUAL REVIEW PROCESS

SOBIR conducts a formal review of this framework each April, alongside the Standard. Minor updates are versioned as point releases (e.g. V2.1). Material changes to criteria or scope are versioned as major releases (e.g. V3.0). Review findings are published at sobir.ca.

B.2 MODEL UNLEARNING STANDARDS

Criterion 1 requires entities to implement documented technical remediation pathways upon consent withdrawal where biometric data has been used in model training. The technical standards for model unlearning are an active area of research. SOBIR will update the normative requirements in Criterion 1 as technically validated standards emerge. Assessors should consider the state of an entity's unlearning capabilities during scoping.

B.3 PROVENANCE MECHANISM ROBUSTNESS

Criterion 2 requires that provenance mechanisms resist removal and manipulation and that robustness be demonstrated through independent testing. The technical methods for testing provenance robustness are developing. SOBIR will refine robustness testing requirements as the field matures. Assessors should engage qualified independent technical reviewers where their own expertise does not cover the specific implementation under review.

B.4 PIPELINE AND MULTI-ENTITY ASSESSMENT

Point-of-contact assessment is the current methodology for multi-entity systems. This approach has known limitations: an entity may be individually compliant while participating in a pipeline that produces harm at another point of contact. Comprehensive pipeline assessment methodology does not currently exist in standardized form. SOBIR will develop guidance on pipeline evaluation in future versions.

B.5 JURISDICTIONAL ALIGNMENT

The Standard sets out its alignment with existing law. Future versions of this framework should map its criteria to major regulatory frameworks, including the EU AI Act, EU GDPR, Canada's PIPEDA, Quebec's Law 25 and Bill 24, applicable US state biometric privacy laws such as Illinois' Biometric Information Privacy Act, and emerging Asia-Pacific frameworks, to assist entities in understanding how these criteria relate to their regulatory obligations.

Intellectual Property Notice: This document is the intellectual property of the Society for Original Biometric Identity Rights. It may be referenced and cited with attribution. It may not be reproduced, adapted, or represented as the work of any other organization without written permission from SOBIR, except as permitted by law, including fair dealing. Version 2.0, November 2026. BC Society No. S0083123. sobir.ca
© 2026 Society for Original Biometric Identity Rights. All rights reserved. First published April 2026.
Correspondence: admin@sobir.ca