



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD

CMOS-SB Standard 0003

Emotional Transparency & Disclosure Standard

ETDS v1.0 | Ratified Date: July 26, 2026 | Status: **Active - Public Comment** | Next Review: July 26, 2027

Field	Value
Standard ID	CMOS-SB-1003
Short Name	ETDS
Version	1.0
Governance Spine Position	Pillar 3 of 5 — Transparency & Disclosure
Issued by	CMOS-SB Standards Committee
Ratified by	Founding Council, July 26, 2026
Published	June 9, 2026 (formal public comment period 7/26/26 -8/26/26)
Author / Architect	Isabelle Anne Thompson
Theoretical Basis	Emotional Epidemiology / Cognitive Mode OS Theory
Publication Set Item	Item 8 of the CMOS-SB Publication Set
Prerequisite Standards	EISS (1001) / CMSS (1002)

Governance Note *ETDS mandates proactive, complete disclosure of all emotional inference capabilities and limitations. Covert emotional influence is explicitly prohibited. ETDS compliance requires prior full compliance with EISS and CMSS.*

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

Table of Contents

1	Purpose and Scope	3
	1.1 Purpose	3
	1.2 Scope	3
2	Theoretical Foundations	4
	2.1 Cognitive Mode OS Theory	4
	2.2 Emotional Epidemiology	4
	2.3 Transparency as Structural Governance	4
3	Transparency Obligation Framework	5
	3.1 Tier 1 — System-Level Disclosure	5
	3.2 Tier 2 — Interaction-Level Disclosure	5
	3.3 Tier 3 — Data-Level Disclosure	5
4	Mandatory Disclosure Requirements	6
	4.1 Capability Disclosure	6
	4.2 Impact Disclosure	6
	4.3 Population-Level Disclosure	7
5	System Capability Disclosure Rules	7
6	Emotional Impact Disclosure Rules	8
7	Data Use Disclosure Rules	9
8	Disclosure Format and Timing Requirements	10
	8.1 Format Requirements	10
	8.2 Timing Requirements	10
9	Prohibited Disclosure Practices	11
	9.1 Dark Patterns	11
	9.2 Vague Language	11
	9.3 Retroactive Disclosure	12
	9.4 Consent Laundering	12

1	Purpose and Scope	3
10	Compliance Checklist	12

Section 1

—

Purpose and Scope

1.1 Purpose

The Emotional Transparency and Disclosure Standard (ETDS), designated CMOS-SB Standard 1003, establishes binding requirements for how systems subject to CMOS-SB jurisdiction must disclose to users the nature, extent, and operational use of any capabilities that may affect their emotional state or cognitive mode. ETDS is a Pillar 3 governance instrument within the CMOS-SB Governance Spine, addressing the Transparency & Disclosure obligation that undergirds the full five-pillar architecture.

Specifically, ETDS requires that all covered systems disclose to users:

1. That the system has capabilities that may affect their emotional state or cognitive mode;
2. What those capabilities are, described in plain and accurate terms;
3. How those capabilities are being used within any given interaction or operational context; and
4. What emotional data or signals the system is collecting, processing, modeling, or acting upon — in real time or in aggregate.

ETDS prohibits opaque emotional influence in all forms. It requires that disclosure be meaningful, timely, and legible at all points of emotional-impact interaction. Disclosure that is technically present but practically unintelligible, buried, or structured to discourage engagement does not satisfy ETDS obligations.

Foundational Principle

Users cannot exercise informed agency over emotional-impact systems they cannot see. ETDS exists to make the invisible visible — and to hold systems accountable for the clarity, accuracy, and completeness of what they reveal.

1.2 Scope

ETDS applies to all systems within CMOS-SB jurisdiction as defined in CMOS-SB Standard 1001 (CMOSF — Cognitive Mode OS Framework Standard). This includes, but is not limited to:

- Artificial intelligence and machine learning systems that interact with human users in real time;
- Digital platforms and applications that use personalization, adaptive content delivery, or behavioral modeling;
- Systems that collect, process, or act upon emotional signals, sentiment data, behavioral patterns, or attention metrics;
- Systems operating at consumer scale that shape information environments in ways that may influence users' emotional states or cognitive modes; and
- Any subsystem, module, or third-party integration that performs emotional-impact functions on behalf of a covered system.

Compliance Prerequisite. ETDS compliance requires prior or concurrent compliance with CMOS-SB Standard 1005 (EISS — Emotional Impact Safety Standard). A system must have completed or be actively engaged in EISS compliance before initiating ETDS self-certification or audit procedures. Systems that have not achieved EISS compliance are not eligible to self-certify under ETDS.

Standard of Compliance. Compliance with ETDS is a continuous obligation, not a one-time certification event. Systems must demonstrate active compliance with all disclosure, format, timing, and prohibited practices requirements set forth herein. Passive or implied disclosure does not satisfy ETDS obligations. Silence, omission, or disclosure-by-reference to general terms of service is insufficient.

Exclusions. Systems that collect no emotional data, perform no emotional inference, and execute no adaptive behavioral functions are not subject to ETDS. Systems seeking exclusion must affirmatively demonstrate exemption eligibility through the CMOS-SB exemption review process. Self-declared exemptions without supporting documentation do not constitute valid exclusion.

Section 2

Theoretical Foundations

2.1 Cognitive Mode OS Theory

Cognitive Mode OS Theory, developed by Isabelle Anne Thompson and forming the theoretical basis of the full CMOS-SB governance architecture, proposes that the human mind operates through a set of dynamic cognitive and emotional modes — each characterized by distinct processing styles, susceptibility profiles, and information reception patterns. These modes are not static personality traits but fluid operational states that shift in response to environmental inputs, interpersonal interactions, and — critically — the design and behavior of the digital and AI systems a person engages with.

Within this theoretical framework, a system that influences a user's emotional state is not merely providing a service — it is intervening at the operating-system level of human cognition. Such intervention carries structural consequences. A system that shifts a user into a high-susceptibility cognitive mode without disclosure, without consent, and without the user's awareness of what has occurred has not merely influenced a preference. It has altered the conditions under which that person makes decisions, processes information, and relates to others.

Cognitive Mode OS Theory therefore holds that emotional transparency is not an optional ethical enhancement layered on top of functionality. It is a structural precondition for legitimate system operation. Without disclosure, the user's cognitive mode cannot be defended. Without a defensible cognitive mode, informed consent is fiction. Without informed consent, governance fails at its foundation.

2.2 Emotional Epidemiology

Emotional Epidemiology, as applied within the Cognitive Mode OS governance framework, treats emotional influence as a population-level phenomenon with measurable transmission dynamics. Just as infectious disease epidemiology models the spread of pathogens through a population — accounting for exposure rates, susceptibility, transmission vectors, and outcomes — Emotional Epidemiology models the spread of emotional states, mood contagion, cognitive drift, and psychological susceptibility through human populations via systemic channels, including digital systems and AI platforms.

Under this framework, a system that operates without transparency does not merely create individual risk. It creates population-level risk. When millions of users are simultaneously exposed to emotional-impact capabilities they cannot see, cannot understand, and have no meaningful opportunity to resist or adjust, the aggregate effect constitutes a measurable public health concern — one with documented consequences for decision-making quality, social cohesion, and individual psychological stability.

Emotional Epidemiology provides ETDS with its population-scale urgency. Disclosure requirements are not merely consumer protection mechanisms for individual users. They are systemic intervention points that, when properly implemented, reduce the population-level transmission of emotional instability driven by opaque systemic influence.

2.3 Transparency as Structural Governance

ETDS situates transparency not as a value preference but as a structural governance requirement — one that enables all other protections in the CMOS-SB framework to function as intended.

The governance architecture of Cognitive Mode OS operates through five interlocking pillars: Framework, Safety, Transparency & Disclosure, Consent, and Enforcement. Each pillar depends on the others. Safety standards (EISS) identify what harms may occur. Consent standards (EDCPS) establish how legitimate authorization is obtained. Enforcement standards define accountability mechanisms. But none of these pillars can function if users cannot see what is being done to them. Transparency is the sensory layer of the governance architecture — without it, users are blind to the interventions being made on their cognitive and emotional states, and no other safeguard can be meaningfully exercised.

Opacity at the Human-Machine Layer is therefore classified under Cognitive Mode OS Theory as a primary risk factor — one that measurably contributes to susceptibility, cognitive drift, emotional instability, and erosion of individual agency. ETDS addresses this risk by mandating disclosure at the system level, the interaction level, and the data level, creating a comprehensive transparency architecture that enables users to see, understand, and respond to the emotional-impact operations being performed upon them.

Section 3

—

Transparency Obligation Framework

ETDS establishes a three-tier transparency obligation framework. Each tier addresses a distinct layer of emotional-impact system operation. Compliance requires active implementation of all three tiers. Compliance with one or two tiers does not constitute full ETDS compliance.

3.1 Tier 1 — System-Level Disclosure

Tier 1: System-Level Disclosure

What the system is and what it can do — made visible at the architectural level, before any user interaction occurs.

Tier 1 requires that systems publish clear, publicly accessible documentation of all emotional-impact capabilities at the system architecture level. This documentation must exist independently of any specific user interaction and must be available to any person — including regulators, researchers, and prospective users — prior to engagement with the system.

Tier 1 disclosures must identify all capabilities that meet the definition of emotional-impact functions under CMOS-SB Standard 1001 (CMOSF), including emotional inference engines, adaptive behavioral response systems, cognitive load modulation features, attention tracking mechanisms, sentiment

analysis components, and any other subsystem that monitors, models, or responds to user emotional or cognitive state signals.

Tier 1 documentation must be updated whenever a material change to emotional-impact capabilities occurs and must carry version history sufficient to establish a clear record of what was disclosed, when, and in what form.

3.2 Tier 2 — Interaction-Level Disclosure

Tier 2: Interaction-Level Disclosure

What the system is doing in a specific interaction — disclosed at the moment of emotional-impact engagement.

Tier 2 requires that systems disclose, at the point of interaction, when they are using emotional-impact capabilities that may affect a user's cognitive mode or emotional state. Interaction-level disclosure is the real-time transparency obligation — it ensures users are informed not merely that a system has certain capabilities in the abstract, but that those capabilities are being engaged in a specific moment that affects them.

Tier 2 disclosures must be timely (at or before the point of impact), non-intrusive in format, accurate in description of what the system is doing and why, and accompanied by clear information about how the user may adjust or opt out of the relevant capability. See Section 6 for detailed interaction-level disclosure rules.

3.3 Tier 3 — Data-Level Disclosure

Tier 3: Data-Level Disclosure

What data the system is collecting and using — disclosed with specificity, accuracy, and recency.

Tier 3 requires that systems disclose what emotional signals, behavioral data, or cognitive mode indicators they are collecting, modeling, or acting upon — whether in real time or in aggregate. Data-

level disclosure addresses the information infrastructure that underlies emotional-impact system operation. Users must be able to understand not only what the system does, but what raw material it uses to do it.

Tier 3 disclosures must identify all categories of emotional and behavioral data collected, describe how such data is processed and used, specify retention periods, indicate whether data is shared and with whom, and explain how users may access, correct, or request deletion of their data. See Section 7 for detailed data use disclosure rules and cross-reference to CMOS-SB Standard 1004 (EDCPS) for consent requirements.

Section 4

—

Mandatory Disclosure Requirements

The following disclosure requirements are mandatory for all systems subject to ETDS jurisdiction. Covered systems must implement all applicable disclosures. Selective implementation — compliance with some mandatory disclosures while omitting others — does not constitute ETDS compliance and may constitute a violation subject to enforcement action under CMOS-SB Standard 1005 (EISS) and applicable enforcement instruments.

4.1 Capability Disclosure

All systems subject to ETDS must disclose, at minimum, the following capabilities if they are present in system design or operation:

#	Capability Category	Required Disclosure Content
4.1(a)	Emotional Inference	Whether the system uses emotional inference; what signals it uses to infer emotional state; how those inferences are generated; and with what degree of confidence or error margin.

#	Capability Category	Required Disclosure Content
4.1(b)	Adaptive Response	Whether the system adapts responses based on emotional signals; what types of adaptations are made; what triggers adaptation; and whether the user can disable or limit adaptive response behavior.
4.1(c)	Cognitive Load Modulation	Whether the system modulates cognitive load; how modulation is implemented (e.g., pacing, complexity adjustment, content filtering); what cognitive mode or state the modulation targets; and how this affects the user experience.
4.1(d)	Attention and Engagement Tracking	Whether the system tracks attention or engagement patterns for optimization purposes; what behavioral signals constitute attention or engagement data; how such data is used; and whether it is used to increase engagement duration or intensity.
4.1(e)	Sentiment Analysis	Whether the system performs sentiment analysis on user inputs; what inputs are analyzed (text, voice, behavioral patterns); how sentiment classifications inform system behavior; and how users may review or challenge sentiment classifications applied to them.
4.1(f)	Personalization Based on Emotional Modeling	Whether personalization decisions are informed by emotional modeling or historical emotional state data; the basis on which personalization profiles are built; and how long such profiles are retained and whether they can be reset.

4.2 Impact Disclosure

At the interaction level, systems must disclose when content, pacing, adaptive responses, or other system behaviors may have a material emotional impact on the user. Impact disclosures must be triggered whenever the system:

- Delivers content that has been selected, sequenced, or filtered based on emotional signals;
- Modulates the pace, complexity, or tone of interaction based on inferred emotional state;
- Activates a high-sensitivity engagement mode (as defined in Section 6.4);
- Responds to a detected or inferred crisis signal, grief indicator, or acute distress marker; or
- Uses emotional state data to determine the type, framing, or sequencing of persuasive content, offers, or calls to action.

Impact disclosures must be honest in characterization. A system must not frame an emotional-impact disclosure in terms that minimize, obscure, or euphemize the nature of what is occurring. Disclosure language must accurately describe what the system is doing and why, in terms a user without technical knowledge can understand.

4.3 Population-Level Disclosure

Systems operating at population scale — defined as systems with one million or more active users in any rolling 12-month period — must disclose aggregate emotional impact patterns in regular public reporting. Population-level disclosure obligations include:

- **Quarterly Aggregate Reporting:** Publication of anonymized, aggregated data on emotional state classifications observed across the user base, including frequency of high-distress signals, high-susceptibility indicators, and crisis-level detections.
- **Annual Impact Assessment:** A comprehensive annual assessment of the system's population-level emotional influence patterns, including any measured or estimated effects on user wellbeing, engagement behavior, and cognitive mode distribution across the user base.
- **Anomaly Disclosure:** Timely public disclosure within 30 days of detection of any population-level emotional impact anomaly — defined as a statistically significant shift in aggregate user emotional state indicators that is attributable to a system design change, algorithmic update, or operational event.

Section 5

System Capability Disclosure Rules

Section 5 establishes detailed rules governing how system capability disclosures required under Section 4.1 and Tier 1 of the Transparency Obligation Framework must be written, maintained, and made

accessible. These rules apply to all static, publicly available capability disclosure documents and to any onboarding materials that serve a capability disclosure function.

5.1 Plain Language Requirement

All system capability disclosures must be written in plain language. Technical terminology may be used only where it is necessary for precision and must always be accompanied by a plain-language explanation. Systems must not use technical obfuscation — the use of technically accurate but practically unintelligible language — as a method of satisfying the letter of disclosure requirements while defeating their purpose.

The maximum permissible reading level for system capability disclosures is Grade 10 (Flesch-Kincaid or equivalent scale). Disclosures targeting consumer audiences must target Grade 8 or below. Systems serving specialized professional audiences may apply for a reading level adjustment through the CMOS-SB review process, with justification.

5.2 Prohibition on Technical Obfuscation

Systems must not use any of the following practices in capability disclosures:

- Excessive jargon, acronym stacking, or technical abstraction without plain-language accompaniment;
- Passive voice constructions that obscure the system's role as the agent of emotional-impact activity (e.g., "emotional signals are processed" rather than "our system processes emotional signals");
- Disclosure documents of excessive length that are practically inaccessible despite being technically available;
- Embedding capability disclosures within general privacy policies, terms of service, or legal agreements in a manner that makes them non-findable without legal expertise; or

- Reliance on external links, nested references, or multi-document disclosure structures that prevent a user from obtaining a complete picture of system capabilities in a single, coherent document.

5.3 Mandatory Inclusion in Onboarding

System capability disclosures must be presented to every new user at or before the point of initial engagement with the system. Onboarding capability disclosure must:

- Summarize all material emotional-impact capabilities in a format that can be read in five minutes or fewer at a normal reading pace;
- Be presented prior to any user action that would result in emotional-impact data collection or emotional-impact system activation;
- Include a clear, affirmative acknowledgment mechanism — not a buried checkbox or a "by continuing you agree" implied consent structure; and
- Be available for re-review at any time through a clearly marked and easily accessible location within the system interface.

5.4 Annual Refresh Requirement

System capability disclosures must be reviewed and, where necessary, updated on an annual cycle. The annual refresh must include a review of all disclosed capabilities against current system architecture and operation to verify accuracy. Where capabilities have changed, disclosures must be updated and re-presented to existing users with a clear notice of what has changed. Annual refresh completion must be documented and, for population-scale systems, reported in the annual impact assessment required under Section 4.3.

5.5 Version History Maintenance

Systems must maintain a complete version history of all system capability disclosure documents, including:

- The full text of each prior version;
- The date each version was published and the date it was superseded;
- A summary of what changed between versions; and
- For population-scale systems, documentation of how changed disclosures were communicated to users and what user acknowledgment was obtained.

Version histories must be retained for a minimum of seven years and must be producible upon request in any CMOS-SB compliance review or enforcement proceeding.

Section 6

—

Emotional Impact Disclosure Rules

Section 6 establishes rules for interaction-level disclosures required under Tier 2 of the Transparency Obligation Framework and Section 4.2 of the Mandatory Disclosure Requirements. These rules govern when, how, and in what form emotional impact disclosures must be delivered during live user interactions.

6.1 Timing — Before or At the Point of Impact

Interaction-level emotional impact disclosures must be delivered at or before the point of emotional-impact interaction. A disclosure that arrives after the emotional-impact event has already occurred does not satisfy ETDS timing requirements. Systems must be designed so that disclosure mechanisms are triggered by the same conditions that activate emotional-impact capabilities — not after those capabilities have operated.

Where technical constraints make real-time pre-impact disclosure impractical, systems may request a timing variance from the CMOS-SB Standards Committee. Variances are narrow exceptions and not a general accommodation. Systems operating under a timing variance must disclose the variance in their

Tier 1 system capability documentation and must implement compensating controls approved by the Standards Committee.

6.2 Format — Non-Intrusive but Visible

Emotional impact disclosures must be visible and legible without being unnecessarily disruptive to the user experience. Systems must balance disclosure visibility with interaction continuity. ETDS does not require that disclosures interrupt or override the user experience — only that they be presented in a manner that a reasonable, attentive user would notice and be able to read without special effort.

Formats that satisfy this requirement may include persistent disclosure indicators, contextual disclosure banners, embedded disclosure statements, or modal disclosures in high-sensitivity contexts. Formats that do not satisfy this requirement include disclosures accessible only through settings menus, footnotes requiring scroll action, or notifications delivered through channels the user is not currently viewing.

6.3 Content — What the System Is Doing and Why

Interaction-level disclosures must communicate, at minimum:

- That an emotional-impact capability is active or has been triggered;
- What specific capability is active (e.g., "This response has been adjusted based on the emotional tone of your recent messages");
- Why the capability has been activated (e.g., "We detected indicators of stress in your input patterns"); and
- What the practical effect on the interaction may be (e.g., "Content pacing has been reduced and resources for support are available").

6.4 User Agency — Adjustment and Opt-Out

Every interaction-level emotional impact disclosure must include, or link directly to, a clear mechanism by which the user may adjust or opt out of the active emotional-impact capability. The adjustment or opt-out mechanism must be:

- Accessible in no more than two user actions from the point of disclosure;
- Functional — disabling or adjusting the disclosed capability in the manner represented; and
- Non-penalizing — the system must not degrade core service quality, impose additional friction, or otherwise discourage users from exercising the opt-out.

6.5 Special Rules — High-Sensitivity Contexts

High-Sensitivity Context Rule

Systems that detect or infer that a user is engaging in a grief, health, crisis, or acute distress context are subject to elevated disclosure obligations. These rules are mandatory and non-waivable in high-sensitivity contexts.

In high-sensitivity contexts — defined as any interaction in which the system has detected or inferred signals associated with grief, health crisis, acute psychological distress, self-harm risk, or similar states — the following additional disclosure rules apply:

- **Immediate Disclosure:** The system must disclose, without delay, that it has detected high-sensitivity signals and that specialized response protocols are active;
- **Clear Capability Statement:** The system must clearly state what it can and cannot do in the detected context — including explicit acknowledgment of its limitations as a machine system;
- **Resource Disclosure:** The system must provide or offer to provide information about human professional resources relevant to the detected context; and
- **Consent Confirmation:** Where the user's cognitive state may be significantly impaired by acute distress, the system must take affirmative steps to confirm that the user understands and

consents to the interaction continuing under the active emotional-impact protocols, in alignment with CMOS-SB Standard 1004 (EDCPS) high-sensitivity consent requirements.

Section 7

—

Data Use Disclosure Rules

Section 7 establishes rules governing disclosure of emotional data collection and use, fulfilling the Tier 3 Data-Level Disclosure obligations of the Transparency Obligation Framework. These rules apply to all forms of emotional data, behavioral data, cognitive mode indicators, and derived data products that a covered system collects, generates, retains, or acts upon.

Cross-Reference: EDCPS

Section 7 governs *disclosure* of data practices. Consent requirements for emotional data collection, processing, and use are governed by CMOS-SB Standard 1004 (EDCPS — Emotional Data Consent and Permission Standard). ETDS and EDCPS compliance obligations are complementary and must both be satisfied for full Pillar 3 and Pillar 4 governance compliance.

7.1 What Data Is Collected

Systems must disclose, with specificity, all categories of emotional and behavioral data they collect. Generic or catch-all descriptions (e.g., "usage data" or "interaction signals") do not satisfy this requirement. Required disclosure includes:

- The precise categories of data collected (e.g., text sentiment scores, response latency patterns, session duration under stress indicators, vocal tone features);

- The collection method for each category (e.g., real-time inference, passive behavioral logging, explicit user input);
- Whether collection is continuous or event-triggered; and
- Whether data collection occurs in background processes not directly visible to the user during normal interaction.

7.2 How Data Is Processed

Systems must disclose how collected emotional data is processed, including:

- Whether data is processed in real time, in batch, or both;
- What models, algorithms, or inference engines process the data;
- Whether processing results in classifications, scores, profiles, or behavioral predictions applied to the user; and
- Whether any processing is performed by third-party systems or vendors — in which case those third parties must be identified by category (and, where practicable, by name).

7.3 How Long Data Is Retained

Systems must disclose specific retention periods for each category of emotional data collected.

Retention disclosures must specify:

- The duration for which raw emotional data is retained;
- The duration for which derived data products (emotional profiles, behavioral scores, classification histories) are retained;
- The retention period for aggregated or de-identified data derived from emotional data; and
- The conditions under which retained data may be extended beyond standard retention periods (e.g., legal hold, research purposes) and how users are notified of such extensions.

7.4 Whether Data Is Shared

Systems must disclose all third-party sharing of emotional data, including:

- Whether emotional data is shared with any third party for any purpose;
- The categories of third parties with whom data is shared (e.g., advertising partners, analytics vendors, research collaborators, affiliated entities);
- The purpose of each sharing arrangement; and
- Whether users may opt out of third-party sharing and, if so, how.

7.5 How Data Informs System Behavior

Systems must disclose how collected and processed emotional data informs system behavior, including:

- What decisions the system makes based on emotional data (e.g., content selection, response adaptation, pacing adjustment, offer targeting);
- Whether emotional data contributes to automated decision-making with material consequences for the user; and
- Whether and how users may request human review of automated decisions informed by emotional data.

7.6 User Data Rights

Systems must disclose how users may exercise the following data rights with respect to their emotional data:

- **Access:** The right to obtain a copy of all emotional data held about them;
- **Correction:** The right to request correction of inaccurate emotional data or erroneous classifications;
- **Deletion:** The right to request deletion of emotional data, subject to legally required retention obligations; and

- **Portability:** The right to receive emotional data in a portable, machine-readable format for transfer to another system or storage by the user.

The process for exercising each of these rights must be clearly described and must be completable by a user without legal or technical expertise. Response timelines for data rights requests must be disclosed and must comply with applicable law.

Section 8

Disclosure Format and Timing Requirements

Section 8 establishes universal format and timing requirements applicable to all disclosures required under ETDS, across all three tiers of the Transparency Obligation Framework. These requirements operate as a floor: category-specific rules in Sections 5, 6, and 7 may impose additional requirements but may not be interpreted to lower the floor established here.

8.1 Format Requirements

All disclosures required under ETDS must meet the following format standards:

Requirement	Standard
Plain Language	Written in plain language at or below an 8th grade reading level for consumer-facing systems; Grade 10 maximum for professional or specialized systems.
Primary Language	Presented in the user's primary language as identified by system settings or user declaration. Where primary language cannot be determined, the system must offer disclosure in the top three languages by user base volume and default to English.
Visual Accessibility	Displayed in a manner that is visually accessible — meaning adequate font size (minimum 11pt equivalent), sufficient color contrast, and not buried in fine print, footnotes, or secondary navigation requiring multiple clicks to access.
Accessible Formats	Available in accessible formats for users with disabilities, including screen-reader-compatible text, audio description, and, for crisis-sensitive disclosures, format alternatives that do not rely solely on visual presentation.

Requirement	Standard
No Dark Patterns	Disclosure presentation must not employ design patterns that direct user attention away from disclosure content, reduce the salience of the disclosure relative to other interface elements, or make disclosure comprehension cognitively difficult by design. See Section 9.1.
Standalone Intelligibility	Each disclosure must be intelligible as a standalone document or statement — meaning a user who reads only that disclosure can understand what is being disclosed without reference to other documents, prior conversations, or background research.

8.2 Timing Requirements

The following timing standards govern when each category of ETDS disclosure must be delivered:

Disclosure Category	Required Timing	Update Trigger and Timeline
System-Level Capability Disclosure (Tier 1)	At or before initial user engagement with the system. Must be presented during onboarding, prior to any emotional-impact data collection or system activation.	Updated within 30 days of any material change to emotional-impact capabilities. Annual review required regardless of whether changes occur.
Interaction-Level Disclosure (Tier 2)	At or before the point of emotional-impact interaction. Disclosure may not be delivered after the triggering capability has already operated.	Updated in real time as triggering conditions change within an interaction. Where conditions shift, disclosure must reflect current state.
Data Use Disclosure (Tier 3)	Before data collection begins. Data use disclosure must precede any collection of emotional data, behavioral data, or cognitive mode indicators.	Updated within 30 days of any material change to data collection practices, processing methods, retention periods, or sharing arrangements.
Population-Level Disclosure (Section 4.3)	Quarterly for aggregate reporting; annually for comprehensive impact assessment; within 30 days for anomaly disclosure.	Regular cycle per schedule. Anomaly disclosures are event-triggered, not scheduled.

Material Change — Definition

For purposes of ETDS timing requirements, a **material change** is any modification to system capabilities, data practices, or operational procedures that a reasonable user would consider significant in evaluating their relationship with the system or their exposure to emotional-impact activities. When in doubt about materiality, systems should err toward disclosure.

Section 9

—

Prohibited Disclosure Practices

Section 9 enumerates practices that are expressly prohibited under ETDS. Engagement in any prohibited practice constitutes a disclosure violation regardless of whether the system is otherwise technically compliant with ETDS disclosure requirements. Prohibited practices discovered during audit will be treated as material violations and referred for enforcement review under applicable CMOS-SB enforcement instruments.

Enforcement Notice

Prohibited disclosure practices are treated as aggravating factors in any CMOS-SB enforcement action. A system found to have satisfied the literal content requirements of a disclosure while employing prohibited practices to undermine its effectiveness may face enhanced enforcement consequences.

9.1 Dark Patterns

Systems must not use design patterns that obscure, discourage, or complicate disclosure comprehension or user response. Prohibited dark patterns in the disclosure context include, but are not limited to:

- **Confirmshaming:** Using emotionally loaded language to discourage users from exercising disclosure-related choices (e.g., "No thanks, I prefer to stay uninformed");
- **Hidden disclosure:** Placement of disclosures in locations that users are unlikely to encounter without deliberate search — including small-print footnotes, secondary pages accessible only through non-obvious navigation, or within long legal documents;
- **Attention misdirection:** Use of design elements (color, size, placement, animation) that direct user attention away from disclosure content and toward acceptance actions;
- **Complexity weaponization:** Presentation of disclosure content in formats of unnecessary length, complexity, or density designed to discourage full reading; and
- **Timed obscuring:** Disclosure windows that auto-dismiss, time out, or scroll past before a reasonable user could complete reading.

9.2 Vague Language

Disclosures must not use vague, euphemistic, or technically imprecise language that conceals the actual nature, extent, or operational reality of emotional-impact capabilities. The following classes of language are prohibited in ETDS-required disclosures:

- **Euphemistic framing:** Describing emotional inference as "understanding you better," emotional data collection as "improving your experience," or adaptive behavioral response as "personalizing content to your preferences" — without explicit and accurate description of what these phrases actually mean in functional terms;
- **Indefinite quantification:** Use of terms like "some," "certain," "various," or "limited" without specificity in contexts where specific, knowable information is available and required;
- **Capability minimization:** Language that systematically understates the sophistication, scope, or emotional impact of disclosed capabilities; and

- **Circular disclosure:** Disclosure language that refers back to itself or to other vague documents without providing substantive information (e.g., "We process your data as described in our data practices, which are outlined in our privacy documentation").

9.3 Retroactive Disclosure

Systems must not disclose emotional-impact capabilities, data practices, or the occurrence of emotional-impact interactions retroactively — meaning after impact has already occurred and without the user's prior knowledge or consent. Retroactive disclosure does not satisfy ETDS's prospective disclosure requirements.

Where a system discovers that a disclosure obligation was not met at the required time — due to technical failure, oversight, or other cause — the system must:

5. Provide the belated disclosure as soon as practicable;
6. Clearly identify the disclosure as belated and explain why the timing requirement was not met;
7. Offer the user a meaningful remedy for the period during which emotional-impact activity occurred without required disclosure; and
8. Report the disclosure failure in the system's next required compliance documentation filing.

9.4 Consent Laundering

Systems must not obtain consent through disclosure structures that do not provide genuine informed choice. Consent laundering — the practice of using technically compliant disclosure and consent mechanisms to generate the appearance of informed consent while structurally preventing users from exercising genuine agency — is prohibited under ETDS as a disclosure violation, in addition to its treatment as a consent violation under CMOS-SB Standard 1004 (EDCPS).

Consent laundering practices prohibited under this Section include:

- Presenting disclosures in a sequence or context that makes refusal practically impossible (e.g., "accept to continue" gates for essential services with no alternative);

- Framing disclosure so that the material content appears only after a user has already committed to an interaction;
- Bundling emotional-impact capability consent with consent for unrelated services or features so that refusal requires forgoing unrelated, necessary functionality; and
- Structuring the disclosure and consent process so that the path of least resistance is acceptance, and the opt-out path requires disproportionate effort, expertise, or navigation.

Section 10

Compliance Checklist

The ETDS Compliance Checklist is a self-assessment instrument for use by covered systems in evaluating their compliance posture against the requirements of this Standard. Completion of this checklist does not constitute CMOS-SB certification and is not a substitute for formal audit, review, or certification processes as established by the CMOS-SB Standards Committee.

Systems must complete this checklist at initial ETDS compliance assessment, following any material change to system capabilities or data practices, and as part of the annual refresh process required under Section 5.4.

Instruction

For each item, mark **Yes** if the requirement is fully implemented and documented, **No** if the requirement is not yet met, or **N/A** if the item does not apply to this system (with documented justification for each N/A designation).

#	Compliance Requirement	Yes	No / N/A
1	Prerequisite — EISS Compliance: System has achieved or is actively engaged in CMOS-SB Standard 1005 (EISS) compliance prior to initiating ETDS certification.	☐	☐
2	Tier 1 — System Capability Disclosure Published: Publicly accessible documentation of all emotional-impact capabilities has been published at the system architecture level and is available to any person prior to engagement.	☐	☐
3	Tier 1 — Plain Language Standard Met: All system capability disclosures meet the applicable reading level requirement (Grade 8 for consumer systems; Grade 10 maximum for specialized systems).	☐	☐
4	Tier 1 — Onboarding Disclosure Active: Capability disclosures are presented to every new user at or before initial engagement, prior to any emotional-impact data collection or system activation.	☐	☐
5	Tier 2 — Interaction-Level Disclosure Active: Mechanisms are in place to deliver interaction-level disclosures at or before the point of emotional-impact interaction for all triggering capability categories identified in Section 4.2.	☐	☐
6	Tier 2 — User Agency Mechanism Functional: Every interaction-level disclosure includes or links to a functional opt-out or adjustment mechanism accessible in no more than two user actions.	☐	☐
7	Tier 2 — High-Sensitivity Context Rules Implemented: Elevated disclosure obligations for grief, health, crisis, and acute distress contexts are implemented and triggered by the conditions specified in Section 6.5.	☐	☐
8	Tier 3 — Data Use Disclosure Accurate and Current: All emotional data collection and use disclosures (Sections 7.1–7.6) are accurate, specific, and reflect current system data practices.	☐	☐
9	Tier 3 — User Data Rights Disclosed and Operational: Users are informed of their access, correction, deletion, and portability rights, and the mechanisms for exercising those rights are functional and documented.	☐	☐
10	Format Requirements Met: All ETDS disclosures meet the format standards set out in Section 8.1, including plain language, primary language delivery, visual accessibility, and accessible format availability.	☐	☐
11	Timing Requirements Met: System-level disclosures are made at or before initial engagement; interaction-level disclosures at the point of impact; data use disclosures before collection begins; and all updates are completed within 30 days of material changes.	☐	☐
12	Prohibited Practices Absent — Dark Patterns: System disclosure design has been reviewed and no prohibited dark patterns (Section 9.1) are present in disclosure presentation.	☐	☐

#	Compliance Requirement	Yes	No / N/A
13	Prohibited Practices Absent — Vague Language: All ETDS disclosures have been reviewed for prohibited vague, euphemistic, or technically imprecise language as defined in Section 9.2.	☐	☐
14	Prohibited Practices Absent — Retroactive Disclosure: No ETDS disclosure has been provided retroactively without the remediation steps required under Section 9.3.	☐	☐
15	Prohibited Practices Absent — Consent Laundering: Disclosure and consent structures have been reviewed and no consent laundering practices identified in Section 9.4 are present.	☐	☐
16	Annual Refresh Completed: All system capability disclosures have been reviewed against current architecture within the past 12 months, updated where necessary, and re-presented to existing users where material changes occurred.	☐	☐
17	Version History Maintained: Complete version history of all ETDS disclosure documents is maintained and retained in accordance with the seven-year minimum retention requirement under Section 5.5.	☐	☐
18	Population-Level Reporting Current (if applicable): For systems with one million or more active users in any rolling 12-month period, quarterly aggregate reporting and annual impact assessment are current and publicly published as required by Section 4.3.	☐	☐
19	Third-Party Sharing Disclosed: All third-party sharing of emotional or behavioral data is disclosed with specificity as required by Section 7.4, including the identity of sharing categories, purpose of sharing, and user opt-out availability.	☐	☐
20	EDCPS Cross-Compliance Confirmed: System has confirmed that ETDS data use disclosures are aligned with consent structures established under CMOS-SB Standard 1004 (EDCPS), and no ETDS disclosure is used as a substitute for required EDCPS consent.	☐	☐

Checklist Completed By: _____ Title: _____

System / Product Name: _____ Date: _____

ETDS Version Assessed Against: CMOS-SB-1003 v1.0 Next Scheduled Review: _____

Certification Notice

Completion of this self-assessment checklist is a prerequisite for formal ETDS compliance submission but does not itself constitute certification. Systems seeking formal CMOS-SB certification under ETDS must submit this completed checklist, supporting documentation for all Yes responses, and remediation plans for all No responses to the CMOS-SB Standards Committee through the formal compliance submission process at cmos-sb.org.

CMOS-SB Standard 1003 — Emotional Transparency and Disclosure Standard (ETDS) v1.0

Published: June 9, 2026 | Effective: June 9, 2026 | Next Review: June 9, 2027

Issued by the CMOS-SB Standards Committee | Ratified by the Pending — Standards Board,
September 9, 2026

Author / Architect: Isabelle Anne Thompson

Theoretical Basis: Cognitive Mode OS Theory

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved. | cmos-sb.org