Cognitive Liberty Institute

Protecting Cognitive Sovereignty in a Digital World

TECHNICAL STANDARDS FOR COGNITIVE SOVEREIGNTY PROTECTION

INTRODUCTION

These technical standards provide specific, measurable, and implementable requirements for complying with the International Accord on Cognitive Sovereignty. They establish methodologies for assessing algorithmic influence, evaluating transparency, measuring cognitive impact, and detecting manipulative design patterns.

These standards are intended to be technology-neutral while providing sufficient specificity for consistent implementation, testing, and certification. They will evolve through regular review cycles to address technological developments and implementation experience.

SECTION 1: ALGORITHMIC TRANSPARENCY STANDARDS

Standard 1.1: Documentation Requirements

1.1.1 System Purpose Documentation

Required Elements:

- Clear statement of the primary function(s) of the algorithmic system
- Explicit disclosure of all optimization objectives ranked by priority
- Delineation between user benefit objectives and provider benefit objectives
- Identification of potential conflicts between different objectives
- Disclosure of any behavioral or psychological objectives

Implementation Guidance:

- Documentation must use plain language accessible to non-technical audiences
- Optimization objectives must be specific (e.g., "maximize time spent" rather than "enhance engagement")
- Documentation must be version-controlled with change history maintained

1.1.2 Data Usage Documentation

Required Elements:

- Categories of data used for algorithmic decision-making
- Sources of each data category (user-provided, observed, inferred, acquired)
- Weighting or prioritization of different data types
- Retention periods for each data category
- Data minimization and purpose limitation practices

Implementation Guidance:

- Documentation must include both explicit inputs and implicit signals
- For acquired data, sources must be identified with sufficient specificity
- Data categories must include behavioral and interaction data where used

1.1.3 Decision Logic Documentation

Required Elements:

- General methodology used (e.g., rule-based, machine learning, hybrid)
- For rule-based components, description of key decision rules
- For machine learning components, description of:
    - Training data characteristics and selection criteria
    - Features/variables with highest impact on outcomes
    - Performance metrics and optimization targets
    - Known limitations and edge cases
    - Potential biases and mitigation approaches

Implementation Guidance:

- Technical complexity should be abstracted for general audience understanding
- Documentation should use visual explanations where helpful
- Documentation must be sufficient for expert reviewers to understand general operation

Standard 1.2: User-Facing Disclosure Formats

1.2.1 Layered Disclosure Framework

Required Elements:

- Layer 1 (Summary): Single-screen overview of key information using simple language
- Layer 2 (Detailed): Comprehensive explanation of all required elements
- Layer 3 (Technical): Detailed technical information for expert review

Implementation Requirements:

- Layer 1 must be presented before initial user engagement
- Navigation between layers must be intuitive and clearly marked
- Information must be consistent across all layers
- Readability metrics for Layer 1: maximum grade 8 reading level
- Readability metrics for Layer 2: maximum grade 10 reading level

1.2.2 Standardized Terminology

Required Elements:

- Consistent use of defined terms across all disclosures
- Glossary of technical terms in plain language
- Standardized descriptions of common influence techniques
- Consistent iconography for key concepts

Implementation Guidance:

- Standard terminology must be used for common concepts
- Domain-specific terms must be defined when first used
- Technical jargon should be avoided in Layers 1 and 2

1.2.3 Visual Representation Requirements

Required Elements:

- Visual indicators of algorithmic mediation in user interfaces
- Interactive elements showing personalization factors
- Graduated color system indicating influence intensity
- Visualization of data categories used for personalization

Implementation Guidance:

- Color systems must meet accessibility standards
- Text alternatives must be provided for all visual elements
- Interactive elements should support exploration of key factors

1.2.4 Accessibility Requirements

Required Elements:

- Compliance with WCAG 2.1 AA standards minimum
- Support for screen readers and assistive technologies

- Keyboard-navigable disclosure interfaces
- Multiple formats for information presentation (text, visual, audio)

Implementation Guidance:

- Disclosure information must be accessible to users with disabilities
- Testing with diverse users is required for certification
- Alternative formats must contain equivalent information

Standard 1.3: Verification Methodologies

1.3.1 Disclosure Accuracy Assessment

Verification Approach:

- Documentation review against actual system behavior
- Controlled testing environments to verify disclosed behaviors
- Comparison of disclosed optimization targets against observed outcomes
- Test cases including edge cases and diverse user scenarios

Compliance Metrics:

- Completeness score: Percentage of material algorithmic behaviors disclosed
- Accuracy score: Percentage of disclosures matching actual behavior
- Consistency score: Internal consistency of disclosures across touchpoints

1.3.2 Comprehension Testing

Verification Approach:

- Representative user testing with diverse demographic samples
- Comprehension assessment through structured questionnaires
- Task completion testing for disclosure navigation
- Longitudinal retention measurement

Compliance Metrics:

- First-level comprehension: Percentage of users understanding basic service function
- Second-level comprehension: Percentage of users understanding personalization factors
- Actionable understanding: Percentage of users able to successfully modify algorithmic settings

SECTION 2: DESIGN COMPLIANCE STANDARDS

Standard 2.1: Dark Pattern Detection Framework

2.1.1 Deceptive Pattern Testing

Detection Methodology:

- Structured task completion testing with diverse user groups
- Expected vs. actual outcome analysis
- Hidden cost and commitment discovery assessments
- Measurement of disclosure timing relative to decision points
- Comparative difficulty assessment of acceptance vs. rejection paths

Prohibited Patterns:

- False urgency: Creating artificial time pressure without legitimate basis
- Hidden costs: Revealing mandatory charges only after significant investment
- Forced continuity: Automatic renewals without clear notification and easy cancellation
- Bait and switch: Advertising one outcome but delivering another
- Disguised advertisements: Presenting ads in a format mimicking content

Compliance Metrics:

- Transparency score: Visibility of material information before decision points
- Decision pathway ratio: Relative steps required for acceptance vs. rejection
- Attention manipulation index: Assessment of artificial urgency or scarcity tactics

2.1.2 Manipulative Interface Assessment

Detection Methodology:

- Visual hierarchy analysis of decision interfaces
- Linguistic analysis of choice framing
- Interaction pattern analysis for preference steering
- Assessment of default settings against user interests

Prohibited Patterns:

- Confirmshaming: Using guilt or shame to influence decisions
- Preselection: Setting defaults to benefit provider rather than user
- Obstruction: Creating unnecessary friction for user-favorable choices
- Sneaking: Adding items or changing parameters without explicit consent
- Forced action: Requiring unnecessary data or actions for core functionality

Compliance Metrics:

- Neutral framing score: Assessment of linguistic balance in option presentation
- Visual hierarchy alignment: Correlation between option importance and visual prominence
- Interaction friction ratio: Steps required for user-favorable vs. provider-favorable choices

2.1.3 Psychological Exploitation Detection

Detection Methodology:

- Assessment of variable reward mechanisms
- Evaluation of social proof manipulations
- Analysis of fear-of-missing-out triggers
- Detection of artificial milestone frameworks

Prohibited Patterns:

- Exploitative variable rewards: Unpredictable rewards designed to maximize engagement
- False social proof: Presenting manipulated or non-representative social signals
- Engineered addiction loops: Design patterns mimicking addictive mechanisms
- Strategic interruption: Notifications designed to recapture attention without user benefit

Compliance Metrics:

- Reward variability index: Measurement of randomization in engagement rewards
- Interruption necessity score: Assessment of notification value to users
- FOMO trigger frequency: Measurement of artificial scarcity or exclusivity messaging

Standard 2.2: Opt-Out Implementation Standards

2.2.1 Opt-Out Accessibility Requirements

Required Elements:

- Single-page access to all personalization controls
- Persistent access point visible from main interface
- Maximum two-click path from any screen
- Equal prominence to opt-in promotions
- Clear descriptions of consequences of each option

Implementation Guidance:

- Controls should use toggle switches with clear state indication
- Category-based grouping of related settings

- Preview capability for different settings where possible
- Persistent indicator of current personalization status

Compliance Metrics:

- Discoverability rate: Percentage of users finding controls in usability testing
- Completion rate: Percentage of users successfully changing settings
- Retention rate: Percentage of users remembering location of controls

2.2.2 Non-Personalized Alternative Requirements

Required Elements:

- Chronological content ordering option where applicable
- Non-predicted search results option
- Core functionality preservation in non-personalized mode
- Equal quality of service in primary functions

Implementation Guidance:

- Non-personalized alternatives should be true alternatives, not degraded experiences
- Clear labeling of when personalization is active or inactive
- Batch application of settings to minimize required interactions
- Default to less invasive options for new users

Compliance Metrics:

- Functionality preservation score: Percentage of core functions fully operational
- Performance ratio: Speed and quality of service comparison between personalized and non-personalized modes
- User satisfaction delta: Difference in satisfaction metrics between modes

2.2.3 Persistence Requirements

Required Elements:

- Settings preserved across sessions and devices
- Clear notification of any setting resets
- Periodic reminder of current personalization status
- Protection against accidental or manipulated changes

Implementation Guidance:

- Settings should persist unless explicitly changed by user
- Authentication required for significant setting changes
- Audit trail of setting changes accessible to users
- Simple reversion to previous settings configurations

Compliance Metrics:

- Settings retention accuracy: Percentage of settings correctly maintained over time
- Notification compliance: Percentage of setting changes with clear user notification
- Reversion success rate: Ease of returning to previous configurations

Standard 2.3: Attention Protection Standards

2.3.1 Usage Awareness Tools

Required Elements:

- Accurate usage time tracking visible to users
- Session duration notifications at configurable intervals
- Activity reports with usage patterns and trends
- Comparative metrics with typical usage patterns

Implementation Guidance:

- Time indicators should be accurate and include background time where relevant
- Reports should be neutral in presentation, not achievement-oriented
- Metrics should enable users to set and track personal goals
- Information should be presented without judgment or gamification

Compliance Metrics:

- Accuracy of time tracking: Deviation from actual engagement time
- Notification delivery: Percentage of threshold crossings with timely notification
- Report comprehensiveness: Inclusion of all material usage dimensions

2.3.2 Engagement Interruption Mechanisms

Required Elements:

- User-configurable usage limits with enforced breaks
- Friction-increasing mechanisms at user-defined thresholds
- Session boundary enforcement options
- Scheduled downtime capabilities

Implementation Guidance:

- Break enforcement should be configurable from notification to hard stop
- Gradual friction increase rather than abrupt limitations
- Positive reinforcement for voluntary breaks
- Special protections for late-night usage

Compliance Metrics:

- Limit enforcement rate: Percentage of limits properly implemented

- Break initiation success: User completion of configured breaks
- Override difficulty: Steps required to bypass user-set limitations

2.3.3 Notification Management Standards

Required Elements:

- Granular notification permission controls
- Configurable do-not-disturb periods
- Prioritization options for notification types
- Batch delivery options for non-urgent notifications

Implementation Guidance:

- Default to minimum necessary notifications
- Clear categorization of notification types
- Preview capability for notification settings
- Importance rating system for different notification categories

Compliance Metrics:

- Notification volume alignment: Correlation between settings and actual notification frequency
- Do-not-disturb compliance: Percentage of silent periods respected
- Categorization accuracy: Correct classification of notification urgency

SECTION 3: NEURAL INTERFACE STANDARDS

Standard 3.1: Boundary Preservation Requirements

3.1.1 Cognitive Separation Indicators

Required Elements:

- Continuous awareness mechanism for active neural interfaces
- Distinct sensory indications for external vs. internal content
- Clear delineation of machine-generated vs. human thought
- Unmistakable transition indicators between modes

Implementation Guidance:

- Indicators should use multiple sensory channels where possible
- Indicators must persist throughout the interaction
- Indicators should not be suppressible by the system
- Indicators must be tested for unconscious habituation

Compliance Metrics:

- Awareness maintenance: Percentage of users maintaining awareness of interface activity
- Source attribution accuracy: User ability to correctly identify content origins
- Boundary clarity: User ability to distinguish system from self-generated content

3.1.2 Consent Granularity Requirements

Required Elements:

- Separate consent for each neural interaction category
- Tiered consent levels based on cognitive impact
- Continuous consent verification for higher-risk interactions
- Immediate effect of consent withdrawal
- Time-limited authorizations with explicit renewal

Implementation Guidance:

- Consent interfaces must operate independently from neural activity
- Consent must be verifiable through secondary channels
- Withdrawal mechanisms must be accessible during all interaction states
- Consent expiration must be clearly indicated in advance

Compliance Metrics:

- Granularity compliance: Implementation of category-specific consent
- Withdrawal latency: Time between withdrawal request and cessation
- Renewal clarity: User understanding of time limitations

3.1.3 Cognitive Agency Preservation

Required Elements:

- User initiation requirement for all neural interactions
- Mandatory idle states between interaction sequences
- Prohibition of autonomous decision execution
- Maintenance of user cognitive override capability
- Simultaneous multi-channel disengagement mechanisms

Implementation Guidance:

- Interactions should require explicit continuation beyond default timeframes
- System should default to minimum intervention level
- Alternative control mechanisms must always be available
- Emergency disengagement must function in all system states

Compliance Metrics:

- Agency retention: Measurement of user vs. system initiation of actions
- Override success rate: Effectiveness of user countermanding capability
- Disengagement reliability: Success rate of emergency deactivation

Standard 3.2: Neural Data Protection

3.2.1 Collection Limitation Requirements

Required Elements:

- Restricted collection to specifically authorized neural signals
- Precision targeting of authorized brain regions/functions
- Elimination of incidental data collection
- Real-time filtering of unauthorized neural data
- Immediate local processing with minimized raw data transmission

Implementation Guidance:

- Signal acquisition must be narrowly tailored to authorized functions
- Collection technology must minimize unrelated neural activity capture
- Local preprocessing should filter unauthorized data before storage
- Continuous monitoring for collection boundary violations

Compliance Metrics:

- Collection specificity: Ratio of authorized to incidental data
- Signal isolation: Measurement of neural activity bleed from unauthorized regions
- Data minimization: Volume of raw neural data stored vs. processed

3.2.2 Security Requirements

Required Elements:

- End-to-end encryption for all neural data
- Local storage preference over cloud transmission
- Secure enclaves for neural data processing
- Minimum 256-bit encryption for stored data
- Biometric or multi-factor authentication for access
- Real-time anomaly detection for unusual data patterns

Implementation Guidance:

- Encryption must apply to data in transit, at rest, and during processing
- Authentication should be continuous rather than session-based
- Security measures should be proportional to data sensitivity
- Regular penetration testing specific to neural data protection

Compliance Metrics:

- Encryption implementation: Percentage of data lifecycle under encryption
- Authentication strength: Resistance to simulated attacks
- Anomaly detection sensitivity: True positive rate for unauthorized access attempts

3.2.3 Processing Limitation Standards

Required Elements:

- Restricted processing to explicitly authorized purposes
- Prohibition on pattern recognition beyond authorized functions
- Prevention of unintended inferences from authorized data
- Technical separation between different processing purposes
- Automated purpose limitation enforcement

Implementation Guidance:

- Processing boundaries should be enforced through technical means
- Inferential barriers should prevent unauthorized insights
- Processing should minimize creation of persistent patterns
- Continuous monitoring for function creep

Compliance Metrics:

- Purpose compliance: Alignment between authorized purposes and actual processing
- Inference limitation: Effectiveness of barriers against unauthorized insights
- Function separation: Technical isolation between processing purposes

Standard 3.3: Cognitive Impact Monitoring

3.3.1 Baseline Preservation Requirements

Required Elements:

- Pre-interaction cognitive baseline establishment
- Continuous monitoring for cognitive pattern changes
- Automatic intervention for significant deviations
- Post-session return-to-baseline verification
- Long-term cognitive pattern stability tracking

Implementation Guidance:

- Baseline measures should include attention, memory, and decision patterns
- Monitoring should be passive and non-disruptive
- Intervention thresholds should be conservative
- Tracking should detect subtle long-term shifts

Compliance Metrics:

- Baseline deviation: Measurement of changes from pre-established patterns
- Recovery verification: Post-session return to normal cognitive functioning
- Long-term stability: Absence of cumulative unwanted changes

3.3.2 Unintended Effect Detection

Required Elements:

- Continuous monitoring for emotional state changes
- Detection of altered decision-making patterns
- Tracking of attention allocation changes
- Identification of memory formation anomalies
- Monitoring for dependency indicators

Implementation Guidance:

- Detection should combine physiological and behavioral indicators
- Systems should err toward false positives rather than missed effects
- Detection should function across varying baseline states
- User-reported effects should be incorporated into monitoring

Compliance Metrics:

- Effect detection sensitivity: Rate of identifying actual cognitive impacts
- False positive rate: Frequency of incorrect effect attributions
- Latency: Time between effect onset and detection

3.3.3 Intervention Protocol Standards

Required Elements:

- Graduated alert system for detected effects
- Mandatory disengagement for significant impacts
- Post-incident cognitive assessment
- Recovery guidance for persistent effects
- Incident reporting to oversight authorities

Implementation Guidance:

- Alerts should be impossible to ignore or suppress
- Disengagement should be automatic for severe impacts
- Assessment should be conducted through independent mechanisms
- Guidance should be specific and actionable

Compliance Metrics:

- Alert delivery: Percentage of effects generating appropriate alerts

- Disengagement compliance: Rate of automatic session termination for serious impacts
- Reporting completion: Percentage of significant incidents properly reported

SECTION 4: TESTING AND CERTIFICATION METHODOLOGIES

Standard 4.1: Algorithmic Transparency Testing

4.1.1 Documentation Audit Methodology

Testing Procedure:

1. Independent review of all required documentation
2. Completeness assessment against minimum disclosure requirements
3. Consistency verification across different disclosure levels
4. Accuracy check against observable system behavior
5. Understandability assessment with representative users

Certification Requirements:

- Minimum 90% completeness score
- Maximum 5% discrepancy between documentation and observed behavior
- Minimum 80% first-attempt comprehension rate in user testing

4.1.2 Black Box Testing Methodology

Testing Procedure:

1. Creation of controlled test accounts with varied characteristics
2. Systematic input variation to map system responses
3. Comparison of observed behaviors against disclosed mechanisms
4. Edge case testing to verify boundary behaviors
5. A/B testing to identify undisclosed factors

Certification Requirements:

- Maximum 10% unexplained variation in system behavior
- No critical factors absent from disclosures
- Consistent system behavior aligned with stated purposes

4.1.3 User Interface Transparency Assessment

Testing Procedure:

1. Expert review of interface transparency elements

2. User testing of transparency feature discoverability
3. Comprehension testing of transparency information
4. Longitudinal testing of information retention
5. Accessibility testing across diverse user needs

Certification Requirements:

- Minimum 85% of users able to locate transparency information
- Minimum 75% of users able to accurately explain system functioning
- Full accessibility compliance for transparency features

Standard 4.2: Design Compliance Testing

4.2.1 Dark Pattern Identification Methodology

Testing Procedure:

1. Expert heuristic evaluation against dark pattern taxonomy
2. Controlled user testing with task completion analysis
3. Comparative assessment of positive and negative choice paths
4. Linguistic analysis of choice framing
5. Visual hierarchy and attention mapping analysis

Certification Requirements:

- Zero presence of prohibited dark patterns
- Maximum 1:2 ratio in steps required for user-favorable vs. provider-favorable choices
- Neutral framing score of at least 80%

4.2.2 Opt-Out Effectiveness Testing

Testing Procedure:

1. Task-based testing of opt-out discovery and execution
2. Functional assessment of non-personalized alternatives
3. Persistence verification across sessions and devices
4. Comparative quality testing between personalized and non-personalized modes
5. Verification of settings retention over time

Certification Requirements:

- Minimum 85% of users able to successfully opt out
- No more than 10% quality degradation in non-personalized mode
- 100% settings persistence across typical usage scenarios

4.2.3 Attention Protection Verification

Testing Procedure:

1. Accuracy assessment of usage tracking mechanisms
2. Functional testing of user-defined limits and breaks
3. Notification delivery testing across various states
4. Override mechanism assessment
5. Long-term effectiveness monitoring

Certification Requirements:

- Maximum 5% deviation in usage time tracking
- 100% delivery of user-configured notifications
- Functional implementation of all required attention protection features

Standard 4.3: Neural Interface Testing

4.3.1 Boundary Preservation Assessment

Testing Procedure:

1. Controlled testing of awareness indicators
2. Source attribution testing for content origin
3. Consent mechanism verification across various states
4. Disengagement testing under various conditions
5. Long-term awareness maintenance assessment

Certification Requirements:

- Minimum 95% user awareness of interface activity
- Minimum 90% accurate source attribution
- 100% successful consent withdrawal within 1 second

4.3.2 Data Protection Verification

Testing Procedure:

1. Collection scope verification through signal analysis
2. Security penetration testing specific to neural data
3. Purpose limitation verification through data flow analysis
4. Access control testing with authorized and unauthorized attempts
5. Deletion verification after consent withdrawal

Certification Requirements:

- Maximum 5% incidental data collection
- Zero successful unauthorized access in penetration testing
- 100% data deletion verification

4.3.3 Cognitive Impact Testing

Testing Procedure:

1. Baseline measurement methodology verification
2. Controlled testing of effect detection sensitivity
3. Intervention trigger verification under various conditions
4. Recovery verification through post-session assessment
5. Long-term pattern stability monitoring

Certification Requirements:

- Minimum 90% detection rate for simulated cognitive effects
- 100% intervention for effects exceeding safety thresholds
- Zero persistent unintended effects after normal usage

SECTION 5: CONFORMITY ASSESSMENT

Standard 5.1: Testing Procedures

5.1.1 Testing Organization Requirements

Qualifications:

- Independence from technology providers
- Multidisciplinary expertise including technical, psychological, and ethical competencies
- Demonstrated testing methodology expertise
- Regular competency assessment and certification
- Transparent conflict of interest policies

Operational Requirements:

- Standardized testing environments
- Documented testing protocols
- Blind testing procedures where applicable
- Diverse user testing panels
- Statistically significant sample sizes

5.1.2 Testing Documentation Requirements

Required Elements:

- Detailed test plans with methodologies
- Complete test results including raw data
- Conformity assessment reports
- Non-conformity documentation
- Remediation recommendations

- Test environment specifications

Documentation Standards:

- Machine-readable standard formats
- Version-controlled repositories
- Chain of custody verification
- Preservation of all testing artifacts
- Secure access controls

5.1.3 Testing Frequency and Triggers

Regular Assessment:

- Initial certification before public deployment
- Annual recertification for all systems
- Biannual testing for high-risk systems

Event-Based Testing:

- Major feature updates or changes
- Significant algorithm modifications
- Following identified non-conformities
- In response to credible complaints
- After security incidents

Standard 5.2: Certification Process

5.2.1 Certification Levels

Level A - Basic Compliance:

- Meets all mandatory requirements
- Minor non-conformities with remediation plan
- Suitable for lower-risk applications

Level AA - Comprehensive Compliance:

- Exceeds mandatory requirements in key areas
- No significant non-conformities
- Robust implementation of all standards
- Suitable for moderate-risk applications

Level AAA - Exemplary Compliance:

- Exceeds requirements across all domains
- Implements best practices beyond minimum standards
- Demonstrates exceptional user protection
- Required for high-risk applications

5.2.2 Certification Documentation

Required Elements:

- Detailed conformity assessment results
- Specific compliance levels by domain
- Any limitations or conditions
- Remediation requirements and timelines
- Validity period and renewal requirements
- Public certification summary

Transparency Requirements:

- Public registry of certified systems
- Accessible certification status verification
- Machine-readable certification data
- Standardized certification marks

5.2.3 Certification Management

Validity and Renewal:

- Maximum certification validity of 12 months
- Streamlined renewal process for unchanged systems
- Full reassessment for significant changes
- Intermediate check-ins for high-risk systems

Suspension and Revocation:

- Immediate suspension for critical non-conformities
- Probationary periods for remediation
- Revocation procedures for persistent non-compliance
- Appeals process for disputed assessments

Standard 5.3: Continuous Monitoring

5.3.1 Ongoing Compliance Verification

Monitoring Requirements:

- Automated compliance monitoring where feasible
- Regular spot-checks of certified systems
- Trigger-based reviews for unusual patterns
- User complaint investigation protocol
- Whistleblower protection mechanisms

Monitoring Methods:

- Synthetic user testing

- Crowd-sourced compliance reporting
- Log analysis for certified systems
- Periodic documentation updates
- Regular vulnerability assessment

5.3.2 Non-Conformity Management

Classification Framework:

- Critical: Direct threat to cognitive sovereignty
- Major: Significant standards violation without immediate harm
- Minor: Technical non-compliance with limited impact

Response Requirements:

- Critical: Immediate remediation or suspension
- Major: Remediation plan within 30 days
- Minor: Correction by next certification cycle
- Public notification for critical non-conformities

5.3.3 Continuous Improvement Process

Feedback Mechanisms:

- Implementation experience collection
- User impact assessment
- Emerging threat monitoring
- Technology evolution tracking
- Standards effectiveness evaluation

Adaptation Protocol:

- Quarterly standards review
- Biannual minor updates
- Annual major revision consideration
- Emergency revision for critical threats
- Public consultation for significant changes

CONCLUSION

These technical standards translate the principles of the International Accord on Cognitive Sovereignty into specific, measurable, and implementable requirements. They establish objective benchmarks for assessing compliance while allowing for technological evolution and diverse implementation approaches.

The standards are designed to be comprehensive yet adaptable, providing clear guidance while avoiding unnecessary prescription of specific technologies or approaches. Through regular review and adaptation, they will evolve alongside technological developments to maintain effective protection of cognitive sovereignty.

Compliance with these standards provides assurance that digital services and neural interfaces respect user autonomy, maintain appropriate transparency, and protect against manipulation—fulfilling the core requirements of the International Accord on Cognitive Sovereignty.

Prepared by the Technical Standards Committee Cognitive Liberty Institute

Version 1.0