



THE HUMAN-SOVEREIGNTY TRANSHUMANISM PROTOCOL STANDARD

A practical standard for evaluating human-enhancement technologies

HERBERT R. SIM

FOUNDING AUTHOR | HSTP-1:2026 | VERSION 1.0 | 28 AUGUST 2026

ORCID: 0009-0008-6500-5749

DOI: 10.5281/zenodo.22211054

Enhance the human - but never surrender the person.

CONTENTS

1. Purpose
2. Scope
3. Normative Language
4. Foundational Principle
5. Core Requirements
6. Human-Sovereignty Red Lines
7. Conformity Assessment
8. Scoring System
9. HSTP Certification Procedure
10. Validity and Reassessment
11. Required Public Disclosure
12. The Human-Sovereignty Test
13. Declaration of HSTP Conformity
14. Relationship to Human-Sovereignty Transhumanism
15. Signature and Version History

EDITION NOTE

This PDF reproduces the public edition of the Human-Sovereignty Transhumanism Protocol Standard in a stable, clean publication format for print, digital reading and permanent scholarly deposit. The online edition remains the reference for subsequent revisions and notices.

Canonical URL: <https://herbertsim.com/human-sovereignty-transhumanism-protocol-standard/>

A technology qualifies as human-sovereign only when it expands human capability without transferring ultimate authority over the person to a government, corporation, algorithm or machine.

- Herbert R. Sim

Document identifier	HSTP-1:2026
Short name	HSTP Standard
Version	1.0
Author	Herbert R. Sim
ORCID	0009-0008-6500-5749
DOI	10.5281/zenodo.22211054
Status	Proposed voluntary certification standard
Original publication date	28 August 2026
Canonical publisher	HerbertRSim.com

Standards-Status Disclaimer

HSTP-1:2026 is a proposed voluntary certification standard authored and published by Herbert R. Sim. It is not a governmental, ISO, IEC, medical, legal or regulatory standard. Publication of the HSTP Standard does not, by itself, certify any technology, product or organization.

1. Purpose

The Human-Sovereignty Transhumanism Protocol Standard - hereafter the HSTP Standard - provides a practical method for determining whether a technology respects the sovereignty of the person who uses it. It translates Human-Sovereignty Transhumanism from a philosophical framework into an assessable system of technical, ethical and institutional requirements. The standard asks not only whether a technology is innovative, effective or safe, but also:

- Who owns the technology?
- Who controls its operation?
- Who owns or controls the data it produces?
- Is adoption genuinely voluntary?
- Can the person refuse it?
- Can the person disconnect from it?
- Can an external party alter or disable it?
- Can automated decisions be challenged?
- Who remains accountable when harm occurs?
- Does the technology expand human agency - or institutional power over the human being?

A technology may improve intelligence, mobility, health, longevity or sensory ability while simultaneously reducing the user's freedom. Technical capability alone is therefore insufficient for HSTP certification.

The HSTP Standard evaluates whether a technology preserves:

- Bodily autonomy
- Cognitive liberty
- Informed and continuing consent
- Mental, genetic, biometric and biological privacy
- Personal control
- Freedom of enhancement
- Freedom of refusal
- Continuity of essential functions

- Transparency and contestability
- Equal human standing
- Institutional accountability
- Effective remedy and redress

This standard is intended for developers, researchers, manufacturers, medical institutions, regulators, investors, employers, insurers, civil-society organizations and individual users.

2. Scope

The HSTP Standard applies to technologies that enter, alter, monitor, support or materially influence the human body, mind, identity, biological inheritance or decision-making process.

Relevant technologies include:

- Brain-computer interfaces
- Neural implants
- Wearable neurotechnology
- Neurostimulation systems
- Cognitive-enhancement technologies
- Artificial-intelligence assistants
- Automated decision systems
- Medical and elective genetic technologies
- Gene-editing systems
- Genetic testing services
- Genomic databases
- Artificial organs
- Advanced prosthetics
- Bionic and robotic limbs
- Exoskeletons and exosuits
- Connected medical devices
- Digital identity systems
- Biometric monitoring
- Emotion-recognition technologies
- Reproductive technologies
- Embryo-selection systems
- Artificial wombs
- Longevity interventions
- Cryonics services
- Digital-continuity services
- Human-robot integration
- Digital replicas of human identity
- Systems that classify enhanced and unenhanced persons

The standard may be applied to:

- A complete product
- An individual component
- A software platform
- A connected service
- A data-processing system
- A medical procedure
- An institutional deployment
- An organization responsible for operating the technology

Certification of one component shall not automatically certify the entire technological system. Every HSTP assessment shall clearly identify its boundaries, including the specific product, version, service, infrastructure and jurisdiction being

evaluated.

3. Normative Language

The following terms establish the level of obligation under the HSTP Standard:

- Shall indicates a mandatory requirement.
- Shall not indicates a prohibited practice.
- Should indicates a strongly recommended practice.
- May indicates an optional practice.
- Conformity means that sufficient evidence demonstrates compliance with a requirement.
- Nonconformity means that a requirement has not been fully satisfied.
- Minor nonconformity means that a limited deficiency exists without immediately threatening fundamental human sovereignty.

- Major nonconformity means that a significant requirement is absent or ineffective.
- Critical nonconformity means that a technology violates a foundational condition of human sovereignty and cannot be certified until the violation is removed. The HSTP Standard evaluates actual practices, not merely stated intentions. A written policy does not establish conformity when the design or operation of the technology contradicts that policy.

4. Foundational Principle

The HSTP Standard is governed by one permanent principle:

Technology may extend human power, but it must not inherit authority over the human person. A conforming technology shall treat the individual as its principal - not merely as a patient, customer, employee, subscriber, data source, biological platform or component of a larger technological system. The person shall remain the primary beneficiary and legitimate authority over technologies integrated with their body or mind. This principle does not require every technology to be owned commercially by its user. Medical equipment, leased devices and institutional systems may involve several legitimate stakeholders. However, no commercial, governmental or institutional arrangement shall deprive a person of meaningful authority

over their:

- Body
- Mind
- Consciousness
- Identity
- Genetic information
- Neural information
- Essential bodily functions
- Fundamental rights
- Legitimate course of development

Technology must remain an instrument through which persons pursue their chosen purposes. It must not become an authority that determines those purposes for them.

5. Core Requirements

HSTP-01: Personal Sovereignty

The technology shall recognize the individual as possessing primary moral authority over their own body, mind, identity and technological development.

The provider shall not claim ownership over:

- The person's body
- The person's brain
- The person's neural activity
- The person's genetic identity

- The person's memories
- The person's involuntary biological processes
- The person's legal or psychological identity
- The person merely because a device has been integrated into them

A manufacturer may retain intellectual-property rights over its technology. Such rights shall not become ownership over the user or over the biological and cognitive activity of the user. A person shall not become the property of an institution because that institution created, financed, enhanced, repaired or maintains part of the person's body.

Required evidence:

- Ownership and licensing terms
- User agreement
- Data-ownership policy
- Statement recognizing bodily and cognitive sovereignty
- Documentation identifying the limits of provider authority

HSTP-02: Freedom of Adoption

Use of the technology shall be voluntary, except where an intervention is medically necessary during an immediate emergency and ordinary consent cannot be obtained. Users shall not be deceived, manipulated or subjected to disproportionate pressure to adopt the technology.

Institutions shall disclose whether refusal will affect access to:

- Employment
- Education
- Healthcare
- Insurance
- Financial services
- Public services
- Social participation
- Other important opportunities

Promotional materials shall distinguish verified benefits from speculation. Marketing shall not exploit fear, disability, economic insecurity or social exclusion to manufacture consent.

Required evidence:

- Consent procedures
- Recruitment materials
- Advertising claims
- Policies governing refusal
- Documentation of available alternatives

HSTP-03: Freedom From Compelled Enhancement

No person shall be forced, manipulated or economically cornered into nonessential technological enhancement. An employer, school, insurer or public institution shall not make invasive enhancement compulsory when a reasonable and less intrusive alternative can achieve the legitimate objective. The existence of a formal refusal option is insufficient when refusal produces severe, unrelated or disproportionate consequences. Enhancement is sovereign only when refusal remains a genuine and sustainable option.

Automatic failure occurs when:

- Enhancement is required as a condition of citizenship
- Invasive neural monitoring is required for ordinary employment without demonstrated necessity
- Refusal results in arbitrary loss of fundamental services
- Consent is obtained through threats, deception or abuse of authority
- Unenhanced persons are denied equal legal standing
- Individuals are punished for refusing experimental intervention

HSTP-04: Informed and Continuing Consent

Consent shall be:

- Specific
- Understandable
- Freely given
- Documented
- Appropriate to the person's capacity
- Renewed when material conditions change
- Capable of withdrawal wherever technically and medically feasible

Consent to one function shall not constitute consent to unrelated future functions. A person who agrees to medical monitoring has not automatically consented to advertising, behavioural profiling, law-enforcement access, political targeting or artificial-intelligence training.

Material changes requiring renewed consent include:

- New data collection
- New third-party access
- New artificial-intelligence functionality
- Changed ownership or control
- New remote-access capabilities
- New behavioural-influence functions
- Expanded medical or commercial uses
- Changes affecting reversibility
- Changes affecting cybersecurity
- New consequences of refusing or disconnecting

Required evidence:

- Plain-language consent form
- Technical consent records
- Consent version history
- Withdrawal process
- Change-notification procedure
- Records demonstrating renewed consent

HSTP-05: Cognitive Liberty

Technologies interacting with the nervous system shall protect freedom of thought, memory, imagination, belief, attention, emotion and perception. The system shall not manipulate cognition or behaviour beyond the functions knowingly authorized by the user.

The technology shall distinguish, where technically possible, between:

- Deliberate commands
- Involuntary neural activity
- Emotional reactions
- Background signals
- Medical indicators
- Inferred intentions
- Confirmed human decisions

Involuntary mental activity shall not automatically be treated as an instruction, agreement, confession or evidence of intent.

Prohibited practices include:

- Undisclosed emotional manipulation
- Forced neurostimulation
- Unauthorized memory modification
- Covert behavioural conditioning
- Punitive use of inferred mental states

- Treating neural predictions as equivalent to deliberate human decisions
- Manipulating political or religious beliefs through undisclosed neurological intervention

The mind shall remain the innermost domain of human sovereignty.

HSTP-06: Mental and Biological Privacy

Neural, genetic, biometric and physiological information shall receive protection proportionate to its intimacy, permanence and potential consequences. The organization shall collect only information necessary for a clearly defined and disclosed purpose. Sensitive human data shall not be sold, transferred, repurposed or used to train artificial intelligence without specific authorization or another clearly disclosed lawful basis compatible with fundamental rights.

The user shall be able to determine:

- What information is collected
- Why it is collected
- Where it is stored
- How long it is retained
- Who can access it
- Whether it leaves the device
- Whether it is combined with other information
- Whether it is used to train artificial intelligence
- Whether new characteristics are inferred from it
- How it may be corrected or deleted

Required safeguards include:

- Data minimization
- Encryption
- Access controls
- Retention limits
- Audit logs
- Breach-response procedures
- Protection against unauthorized inference
- A clear deletion or anonymization process

Mental data shall not be treated as ordinary consumer data.

HSTP-07: Meaningful Human Control

Systems affecting life, liberty, cognition, bodily integrity or fundamental opportunity shall remain subject to meaningful human control.

Human control is meaningful only when the responsible person:

- Possesses adequate information
- Has sufficient time to intervene
- Understands the material consequences
- Can reject the system's recommendation
- Can stop or modify the action
- Can obtain additional review
- Is accountable for the resulting decision

A nominal "human in the loop" does not satisfy this requirement when that person merely approves an opaque or predetermined outcome.

Where appropriate, the system shall provide:

- Manual override
- Safe shutdown
- Emergency disconnection
- Human authorization
- Reversion to a safe state
- Independent review

- An auditable record of consequential actions

The more deeply a technology enters the human body or mind, the stronger the requirement for meaningful human control shall become.

HSTP-08: Right to Disconnect

A connected enhancement shall provide a safe method of disconnection whenever technically and medically possible.

The provider shall disclose:

- Which functions require connectivity
- What happens when connectivity is lost
- Whether the device can operate offline
- Whether an external party can restore connectivity
- Which functions may be remotely changed
- Whether disconnection creates medical risks
- Which information remains stored after disconnection
- Whether monitoring continues while the user is offline

Nonessential network dependence shall not be designed into essential bodily functions merely to create commercial control. A person shall not be punished for disconnecting from optional monitoring, except where the absence of necessary information prevents delivery of a specifically requested service.

HSTP-09: Security by Design

Technologies integrated with the body or mind shall be protected as critical human infrastructure.

Security shall be incorporated throughout the system's lifecycle:

- Design
- Development
- Testing
- Deployment
- Maintenance
- Updating
- Decommissioning
- Removal
- Transfer

The provider shall maintain procedures for:

- Vulnerability reporting
- Security testing
- Security updates
- Authentication
- Unauthorized-access prevention
- Incident investigation
- User notification
- Recovery of safe operation
- Protection against malicious remote control

The organization shall not deliberately weaken security to create unnecessary surveillance access or commercial dependence. A known critical vulnerability capable of compromising bodily or cognitive integrity constitutes a critical nonconformity.

HSTP-10: Transparency and Comprehensibility

Users shall receive a meaningful explanation of how the technology affects them.

The explanation shall include:

- The intended purpose
- Principal functions
- Known risks

- Material uncertainties
- Data practices
- External dependencies
- Remote-control capabilities
- Artificial-intelligence involvement
- Conditions that may cause malfunction
- Procedures for obtaining assistance
- Procedures for obtaining redress

Transparency does not require unrestricted publication of every trade secret. It does require sufficient information for users, auditors and regulators to evaluate safety, control and human-rights consequences. A system that cannot be meaningfully explained shall not independently determine consequential outcomes affecting a person.

HSTP-11: Contestability and Human Appeal

A person shall be able to challenge a consequential technological decision.

This requirement applies when a system influences:

- Medical treatment
- Employment
- Education
- Insurance
- Credit
- Legal status
- Access to public services
- Freedom of movement
- Reproductive decisions
- Bodily intervention
- Cognitive intervention
- Continued operation of an essential enhancement

The appeal process shall be accessible, timely and conducted by a competent human authority capable of changing the outcome. An automated rejection followed only by another automated review does not constitute human appeal. The person shall receive a meaningful explanation of the decision and the evidence upon which it was based, subject to proportionate protection of other persons' rights.

HSTP-12: Personal Data Access and Portability

Users shall have reasonable access to information generated by their own bodies, minds and devices. Where technically feasible, this information shall be exportable in a secure and usable format. The provider shall not use deliberate incompatibility to make departure from its system practically impossible.

Portability should include:

- Relevant health data
- Device settings
- Calibration records
- Neural records
- Genetic or biometric records
- User-generated information
- Consent history
- Operational logs necessary for continuity

Portability may be limited where release would create a serious security risk or expose another person's protected information. Any limitation shall be documented, proportionate and open to review.

HSTP-13: Interoperability and Freedom From Lock-In

Technologies integrated into essential bodily or cognitive functions should support interoperability with safe and qualified alternatives. A person should not become permanently dependent upon one corporation for the continued operation of their own body. Where full interoperability is medically or technically unsafe, the provider shall document

the reason and offer

reasonable pathways for:

- Maintenance
- Replacement
- Transfer
- Data migration
- Safe removal
- Long-term support
- Transition to another qualified provider

Commercial preference alone is not sufficient justification for permanent bodily lock-in.

HSTP-14: Continuity of Essential Function

Essential functionality shall not disappear solely because of:

- Manufacturer bankruptcy
- Corporate acquisition
- Subscription cancellation
- Product discontinuation
- Server shutdown
- Contractual disagreement
- Expiration of an unrelated service
- A change in corporate policy

Providers of essential implanted or integrated technologies shall maintain a continuity plan.

The plan should include:

- Offline or safe operating modes
- Source-code or technical escrow where appropriate
- Replacement arrangements
- Transfer of maintenance responsibilities
- Advance notice of discontinued support
- Safe removal procedures
- Access to necessary medical and technical records

A provider shall not remotely disable an essential bodily function merely to enforce a commercial payment dispute.

HSTP-15: Identity and Legal Continuity

Technological enhancement shall not remove a person's legal identity, citizenship, property, contractual rights or moral standing. The use of artificial organs, prosthetics, neural interfaces, genetic modifications or machine-assisted cognition shall not cause the user to be classified as property or as a non-person. Digital replicas, personality simulations and artificial-intelligence models trained upon a person's communications shall not automatically acquire the identity, rights or authority of the original person.

The organization shall distinguish clearly between:

- The biological or technologically enhanced person
- The person's data
- A digital model of the person
- A legally authorized representative
- An autonomous artificial system

Technological transformation shall not become identity confiscation.

HSTP-16: Equal Standing and Nondiscrimination

Enhanced and unenhanced persons shall retain equal fundamental rights. The technology shall not be designed or deployed to establish legally superior and inferior classes based on enhancement status. Organizations shall assess whether their systems discriminate against individuals based on:

- Disability

- Enhancement status
- Genetic characteristics
- Neural characteristics
- Biological origin
- Refusal of optional monitoring
- Use of competing technologies
- Inability to afford enhancement

Greater intelligence, strength, longevity or technological integration shall not become the basis of a hereditary or engineered ruling class. Different capabilities do not justify unequal moral standing.

HSTP-17: Protection of Children and Vulnerable Persons

Technologies affecting children or persons with limited decision-making capacity shall meet a heightened standard of protection. Authorization by a parent, guardian, employer, physician or state does not eliminate the interests and developing autonomy of the affected person.

The deployment shall consider:

- Necessity
- Proportionality
- Reversibility
- Long-term effects
- The person's assent
- Future freedom of choice
- Risks of dependency
- Risks of discrimination
- Risks of institutional coercion

Nontherapeutic and irreversible interventions affecting children require exceptional justification and independent ethical review. Where possible, interventions should preserve the person's future ability to reconsider, modify or discontinue the technology upon reaching decision-making capacity.

HSTP-18: Intergenerational Responsibility

Technologies capable of affecting future generations shall be assessed according to a higher standard of evidence and accountability.

Relevant interventions include:

- Heritable genetic modification
- Reproductive selection
- Artificial gestation
- Persistent biological agents
- Self-propagating technological systems
- Systems capable of influencing humanity's evolutionary direction

The assessment shall consider:

- Irreversibility
- Heritability
- Long-term uncertainty
- Effects on human diversity
- Effects on future autonomy
- Possibility of biological caste formation
- Environmental consequences
- Monitoring across generations
- Availability of less irreversible alternatives

The inability of future persons to consent does not eliminate present responsibility toward them. Present enhancement shall not be purchased by mortgaging the sovereignty of those yet to be born.

HSTP-19: Accountability and Traceability

Every consequential technological action shall remain traceable to identifiable persons or institutions.

Accountability shall not disappear into:

- An algorithm
- A chain of contractors
- Proprietary secrecy
- Distributed automated systems
- An artificial-intelligence model
- A contractual disclaimer

The organization shall maintain records identifying:

- Who designed the system
- Who approved its deployment
- Who controls its operation
- Who receives its data
- Who is responsible for maintenance
- Who investigates incidents
- Who can interrupt consequential actions
- Who compensates affected persons

No harmful outcome shall be dismissed merely by declaring that “the algorithm decided.” The greater the power of a technology, the clearer the line of accountability shall be.

HSTP-20: Remedy and Redress

People harmed by the technology shall have access to effective remedies.

Depending upon the nature of the harm, remedies may include:

- Explanation
- Correction
- Restoration of function
- Data deletion
- Reversal of an unauthorized change
- Replacement
- Medical support
- Compensation
- Independent review
- Suspension of the technology
- Regulatory appeal
- Judicial appeal

User agreements shall not eliminate all meaningful remedies for negligence, deception, unauthorized experimentation or foreseeable violations of bodily and cognitive integrity. Remedies shall be accessible in practice, not merely described in legal documentation.

6. Human-Sovereignty Red Lines

The following practices constitute absolute prohibitions under the HSTP Standard. A technology engaging in any of these practices shall not receive HSTP certification:

1. Nonconsensual alteration of cognition, memory or emotion outside a narrowly defined medical emergency
2. Forced nontherapeutic enhancement
3. Secret neural, genetic or biometric surveillance
4. Ownership claims over a person’s thoughts, memories or biological identity
5. Remote disabling of an essential bodily function for commercial leverage
6. Undisclosed behavioural manipulation
7. Discrimination that removes fundamental rights based on enhancement status
8. Irreversible intervention upon a person who cannot consent without exceptional necessity and independent

authorization

9. Automated decisions over life, liberty or bodily integrity without meaningful human review
10. Retaliation against users who withdraw optional consent
11. Treating involuntary neural activity as legally equivalent to conscious intention
12. Concealing a known vulnerability capable of compromising bodily or cognitive control
13. Using enhancement to impose political, ideological or religious conformity
14. Creating legally superior and inferior classes of persons according to technological or genetic status
15. Secretly repurposing intimate human data for surveillance, manipulation or artificial-intelligence training

These prohibitions cannot be overcome through additional scoring elsewhere in the assessment. A Human-Sovereignty Red Line results in automatic rejection until the practice has ceased, its consequences have been remedied and the system has been independently reassessed.

7. Conformity Assessment

An HSTP assessment shall examine five categories of evidence.

7.1 Documentary Evidence

Documentary evidence may include:

- Policies
- Contracts
- User agreements
- Consent materials
- Technical documentation
- Security procedures
- Data-flow records
- Governance documents
- Continuity plans
- Incident-response plans

7.2 Technical Evidence

Technical evidence may include:

- System architecture
- Access controls
- Encryption
- Offline functions
- Override mechanisms
- Audit logs
- Portability tools
- Security-testing results
- Remote-access controls
- Data-deletion mechanisms

7.3 Operational Evidence

Operational evidence may include:

- Actual organizational practices
- Staff responsibilities
- Incident handling
- User-support procedures
- Response times
- Third-party relationships
- Maintenance practices

- Records of consent withdrawal

7.4 User Evidence

User evidence may include:

- User interviews
- Complaints
- Withdrawal experiences
- Accessibility assessments
- Records of disputed decisions
- Experiences of refusing enhancement
- Evidence of practical coercion
- Reports of malfunction or dependency

7.5 Independent Evidence

Independent evidence may include:

- External audits
- Penetration testing
- Clinical evaluation
- Regulatory findings
- Peer-reviewed research
- Civil-society assessments
- Independent ethical review
- Independent user-rights evaluation

Written policies alone are insufficient when actual practices contradict them.

8. Scoring System

Each of the twenty core requirements shall receive one of the following scores:

Score	Meaning
0	Not addressed or fundamentally violated
1	Minimal or largely ineffective protection
2	Partial conformity with significant deficiencies
3	Substantial conformity with limited deficiencies
4	Full conformity supported by evidence
5	Exemplary protection exceeding the basic requirement

The maximum score is 100 points.

HSTP Certification Levels

Certification Level	Score	Meaning
HSTP-Rejected	0-49	The technology materially threatens human sovereignty
HSTP-Transitional	50-69	Significant improvements are required
HSTP-Conformant	70-84	Core requirements are substantially satisfied
HSTP-Advanced	85-94	Strong human-sovereignty protections are demonstrated
HSTP-Sovereign by Design	95-100	Human sovereignty is integrated throughout the system

A numerical score cannot compensate for a Human-Sovereignty Red Line. Any automatic-failure condition results in HSTP-Rejected status until the condition has been corrected and independently reassessed.

For HSTP-Conformant status or higher:

- Every core requirement shall score at least 2.
- Consent, cognitive liberty, privacy, human control and security shall each score at least 3.
- No critical nonconformity may remain unresolved.
- No Human-Sovereignty Red Line may be present.
- The assessment boundary shall be publicly disclosed.

9. HSTP Certification Procedure

9.1 Certification Authority and Assessment Type

HSTP conformity may be established through:

1. Self-assessment - conducted by the organization responsible for the technology.
2. Independent assessment - conducted by an assessor institutionally separate from the technology provider.

Every conformity report shall state:

- Assessment type
- Name of assessor
- Assessor's organization
- Material conflicts of interest
- Assessment boundary
- Evidence reviewed
- Date of assessment

A self-assessed organization shall not describe itself as “independently HSTP-certified.” Independent certification may be claimed only when the assessor is separate from the technology provider, discloses material conflicts of interest and publishes sufficient evidence to support the result. Publication of the HSTP Standard does not, by itself, certify any technology, product or organization.

9.2 Certification Process

An organization seeking certification should complete the following process.

Step 1: Define the Assessment Boundary**Identify:**

- The product or system
- The version
- The operator
- The supporting infrastructure
- The relevant jurisdiction
- The intended users
- The purpose of deployment

Step 2: Complete the Initial HSTP Assessment

The organization shall answer every requirement and provide supporting evidence. Unsupported declarations shall not be treated as conformity.

Step 3: Map the Technology's Power Structure**Identify who:**

- Owns each component
- Controls its operation
- Can update it
- Can monitor it
- Can disable it
- Can access its data
- Can alter its functionality

- Is accountable for its consequences

Step 4: Map Human Data Flows

Record:

- What information is collected
- Where it originates
- Where it travels
- Where it is stored
- Who can access it
- How long it is retained
- Whether it is used for secondary purposes
- Whether artificial intelligence is trained upon it

Step 5: Conduct Technical and Governance Review

Test the technology's controls rather than accepting written policy statements alone.

The review should examine:

- Consent
- Access control
- Security
- Disconnection
- Portability
- Human override
- Continuity
- Accountability
- Appeal
- Redress

Step 6: Consult Affected Users

Determine whether the following protections function in practice:

- Informed consent
- Refusal
- Withdrawal
- Portability
- Disconnection
- Human appeal
- Complaint handling
- Remedy

Step 7: Record Nonconformities

Each deficiency shall be classified as:

- Minor
- Major
- Critical

Every nonconformity shall identify:

- The requirement affected
- The evidence
- The potential human impact
- The responsible organization
- The required corrective action
- The deadline for correction

Step 8: Complete Remediation

The organization shall correct deficiencies and provide evidence of the changes. Critical nonconformities shall be resolved before certification.

Step 9: Issue an HSTP Conformity Report

The report shall publish:

- The numerical score
- The certification level
- The assessment boundary
- Material limitations
- Identified nonconformities
- Corrective actions
- Assessment date
- Expiry date
- Identity of the assessor

Step 10: Maintain Continuing Conformity

The organization shall monitor the system and initiate reassessment following significant changes or incidents. Certification is not permanent permission. It is a continuing obligation.

10. Validity and Reassessment

HSTP certification should remain valid for no longer than two years.

Earlier reassessment is required following:

- A major software change
- A major hardware change
- A new category of data collection
- A new secondary use of data
- A significant security incident
- A change of corporate ownership
- Introduction of new artificial-intelligence capabilities
- Expansion into a new high-risk use
- Regulatory action
- Evidence that consent is no longer meaningful
- Evidence that refusal is no longer practical
- Material changes to remote-control functionality
- Material changes to offline operation
- Discovery of previously undisclosed risks

Certification applies only to the identified product, version and assessment boundary. An organization shall not imply that certification covers unrelated products, later versions or its entire corporate conduct.

11. Required Public Disclosure

A certified organization shall publish a concise HSTP conformity statement containing:

- Product or system name
- Version assessed
- Certification level
- Numerical score
- Assessment date
- Expiry date
- Assessment boundary
- Identified limitations
- Unresolved minor nonconformities

- Name of the assessor
- Link to the complete conformity report

Suggested conformity statement [Technology name and version] was assessed under the Human-Sovereignty Transhumanism Protocol Standard HSTP-1:2026 and achieved [certification level] with a score of [score]/100. Certification applies only to the defined assessment boundary and remains valid until [date], unless a material change triggers earlier reassessment. HSTP certification shall not be described as government approval, medical authorization or proof that a technology is entirely free from risk.

12. The Human-Sovereignty Test

Before adopting or certifying any intimate technology, every person and institution should ask:

1. Who owns the technology?
2. Who controls its operation?
3. Who owns or controls the data it produces?
4. Is adoption genuinely voluntary?
5. Can the individual refuse without disproportionate punishment?
6. Can the person disconnect or withdraw consent?
7. Can an external party alter or disable the technology?
8. Can the user understand and challenge consequential decisions?
9. What happens if the provider disappears?
10. Who is accountable when harm occurs?
11. Are enhanced and unenhanced people treated as moral and legal equals?
12. Does the technology increase the person's freedom - or primarily increase the system's power over the person?

If these questions cannot be answered clearly, the technology is not ready to govern an intimate part of human life. If control consistently flows toward governments, corporations or artificial intelligence rather than the individual, the system has crossed from enhancement into administration.

13. Declaration of HSTP Conformity

An organization claiming conformity with the HSTP Standard should make the following declaration:

1. We affirm that the purpose of technology is to expand human capability without extinguishing human agency.
2. We recognize the individual as the sovereign authority over their own body, mind and identity.
3. We shall protect the freedom to enhance and the equal freedom to remain unenhanced.
4. We shall obtain informed and continuing consent.
5. We shall protect neural, genetic, biometric and bodily information.
6. We shall preserve meaningful human control, the right to disconnect and the right to appeal.
7. We shall not convert bodily dependence into commercial or political obedience.
8. We shall protect children, vulnerable persons and future generations from irresponsible or coercive intervention.
9. We shall remain identifiable and accountable for the technologies we create and deploy.
10. We accept that technological power is legitimate only while it remains subordinate to human sovereignty.

14. Relationship to Human-Sovereignty Transhumanism

The HSTP Standard is the 2026 practical implementation instrument of Human-Sovereignty Transhumanism, a philosophy first publicly formulated in 2014.

The philosophy establishes the governing principle:

The human person must remain the sovereign subject of technological progress - never its object, product or property. The Twelve Axioms establish its permanent ethical foundation. The Manifesto declares its public commitments. The HSTP Standard converts those commitments into assessable requirements.

Together, they form a complete progression:

Philosophy -> Axioms -> Manifesto -> Protocol Standard -> Assessment -> Accountability The HSTP Standard does not oppose artificial intelligence, genetics, robotics, neurotechnology, longevity science or human enhancement. It establishes the conditions under which those technologies may legitimately serve humanity. Its objective is not to keep technology weak. Its objective is to keep humanity sovereign.

15. Signature and Version History

Founding Author

Herbert R. Sim
Originator of Human-Sovereignty Transhumanism

Document Record

Document title	The Human-Sovereignty Transhumanism Protocol Standard
Document identifier	HSTP-1:2026
Short name	HSTP Standard
Version	1.0
Author	Herbert R. Sim
ORCID	0009-0008-6500-5749
DOI	10.5281/zenodo.22211054
Status	Proposed voluntary certification standard
Original publication date	28 August 2026
Canonical publisher	HerbertRSim.com
Canonical URL	https://herbertrsim.com/human-sovereignty-transhumanism-protocol-standard/
Associated philosophy	Human-Sovereignty Transhumanism
Associated charter	The Twelve Axioms of Human-Sovereignty Transhumanism
Associated declaration	The Human-Sovereignty Transhumanist Manifesto
Licence	Creative Commons Attribution 4.0 International (CC BY 4.0)

Version History

Version 1.0 - 28 August 2026 First public edition. Establishes the scope, twenty conformity requirements, Human-Sovereignty Red Lines, evidence requirements, scoring methodology, certification levels and declaration of conformity. Future revisions shall preserve a publicly accessible version history. Any change affecting certification thresholds, mandatory requirements, core definitions or Human-Sovereignty Red Lines shall require a new numbered edition. Minor typographical corrections may be recorded without creating a new substantive edition.

Recommended Citation

Sim, Herbert R. (2026). *The Human-Sovereignty Transhumanism Protocol Standard: A Practical Standard for Evaluating Human-Enhancement Technologies* (Version 1.0). HerbertRSim.com.
<https://doi.org/10.5281/zenodo.22211054>

Copyright and Licence

© 2026 Herbert R. Sim. This work is licensed under the Creative Commons Attribution 4.0 International Licence (CC BY 4.0).

Enhance the human - but never surrender the person.

- Herbert R. Sim