CRITICAL PATH INSTITUTE	**Policy**	
	Department: Governance, Risk, and Compliance	
	Title: Global Privacy Policy	
Revision Number: 2.1	**Document #:** GRC-POL-0018	**Date:** 09/02/2025
Review Frequency: Annually	**Document Owner:** Data Protection Officer	

1. PURPOSE

C-Path, including its affiliates and subsidiaries (collectively "C-Path" or the "Company") collects and uses certain information about individuals ("personal data"), including contributors, members, suppliers, business contacts, employees and others, as needed to conduct its activities. C-Path has developed and implemented the Global Privacy Policy ("Policy") to establish a framework for C-Path and its employees to protect the privacy of personal data and comply with applicable data privacy laws and requirements globally.

This Policy sets forth requirements for the use and governance of personal data, to ensure that personal data is being collected, shared and used in appropriate ways, and that individual privacy rights are protected. This Policy should be read in conjunction with the C-Path Information Security Policy, which sets forth the technical and organizational measures for the protection of information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

2. SCOPE

This Policy governs the processing of all personal data that is collected or processed by C-Path. This Policy also applies to all persons who have access to the personal data under the authority of C-Path, including full time employees, part time employees, temporary employees, interns, contractors, and certain others operating within C-Path with access to personal data (collectively "Employees").

This Policy is designed to comply with the various data privacy laws globally, including: US federal privacy laws, US state privacy laws, the European General Data Protection Regulation (GDPR), and any other applicable laws governing the Company's activities in the countries in which it operates.

Certain countries may have more stringent laws with respect to the processing of certain types of data. The relevant local/national law will take precedence in the event that it conflicts with or imposes more stringent requirements than this Policy. In such cases, C-Path will develop additional policies and procedures to comply with local laws. If a contributory/customer/vendor seeks to impose more stringent requirements than those in this policy, this should be addressed by the Data Protection Officer (DPO) who must notify and consult with Information Security, the Privacy Team, and the Legal Department.

Violations of this policy may result in severe civil and criminal penalties and disciplinary action that may lead to a termination of employment, personal liability, or criminal prosecution.

3. DEFINITIONS

a. Data Controller: A person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

b. Data Processing: Any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, alignment or combination, restriction, erasure or destruction.

c. Data Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

d. Data Subject: an identified or identifiable natural person to whom personal data relates.

e. Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the identity of that natural person; examples of personal data include: name, email address, phone number, IP address**.**

f. Sensitive Personal Data: personal data that relates to health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic data, biometric data, criminal records, unique identifiers such as social security number/social insurance number/passport number (or similar), financial information such as bank account number, credit card number; PHI under HIPAA and non-public financial information under GLBA also fall under this category. Processing of sensitive data that relates to criminal convictions and offences of a data subject generally requires specific legal justification under relevant local laws

4. ROLES AND RESPONSIBILITIES

a. **All Personnel:**

i. Data privacy is an obligation of every employee. All individuals working for or with C-Path—including employees, contractors, consultants, interns, and temporary staff—are responsible for ensuring that personal data is collected, stored, handled, and processed appropriately in accordance with this Policy, data privacy principles, and applicable laws.

ii. Responsibilities include:

1. Actively supporting C-Path's privacy objectives.
2. Complying with all privacy policies, processes, and procedures.

b. Privacy Organization

i. **Data Protection Officer (DPO)**

1. C-Path appoints a Data Protection Officer (DPO) where required by law. The DPO is independent and reports to an appropriate management level to ensure effective governance of privacy risks.

2. The DPO, supported by the Privacy Team, is responsible for:
    a. Developing, implementing, maintaining, and improving the organization-wide privacy program.
    b. Identifying and interpreting applicable privacy laws and regulatory requirements.
    c. Maintaining and reviewing this Policy annually and after material changes in business practices.
    d. Developing procedures to implement this Policy.
    e. Managing privacy issues, complaints, and data subject requests.
    f. Developing and maintaining privacy awareness training.
    g. Providing implementation guidance across business units.
    h. Advising on and conducting data protection impact assessments (DPIAs) with Information Owners.
    i. Identifying privacy risks and recommending controls or treatments.
    j. Reporting annually (or as needed) to Senior Management or the Board on privacy activities and compliance status.
    k. Cooperating with supervisory authorities.
    l. Maintaining a processing register of all C-Path personal data activities.

ii. **Privacy Team:**

1. Under the direction of the DPO, the Privacy Team:
    a. Administers the privacy program.
    b. Coordinates with Information Security (InfoSec), IT, Legal, Risk Management, and Information Owners to ensure effective implementation and compliance.

iii. **General Counsel**

1. Demonstrates commitment to the global privacy program.
2. Ensures appropriate allocation of resources for compliance with privacy requirements.

c. Company-Wide Operational Roles

i. Information Owners

1. Typically senior management or designated leads, Information Owners:
    a. Assign classification levels to data assets.
    b. Ensure proper handling of data consistent with this Policy.

c. Conduct risk assessments for the information assets under their responsibility.

d. Collaborate with Information Custodians to apply suitable data protection controls.

e. Periodically review and approve data access rights.

ii. **Information Custodians**

1. Custodians are responsible for operational data protection and system-level safeguards:

a. Understand how data is stored, processed, and transmitted.

b. Implement and maintain physical, technical, and procedural safeguards.

c. Manage access provisioning and de-provisioning in line with authorization.

d. Support Information Owners in risk assessment and mitigation.

e. Monitor access and use of data and associated systems.

5. REVIEWS AND APPROVALS

a. **Document author is:** Data Protection Officer (DPO)

b. **Document owner is:** Data Protection Officer (DPO)

c. **Final approval of this document is given by:** Chief Executive Officer

d. **Document must be reviewed by:**

i. Chief Operating Officer

ii. Data Protection Officer

iii. Privacy Team

1. Chief Technology Officer
2. Director, Information Technology
3. Director, Information Systems and Security
4. ISMS Manager

e. **This document is to be reviewed:** At least annually, or whenever there is a material change in business practices, a regulatory update, an incident, or an audit finding impacting the processing of personal data

6. POLICY

a. PRIVACY PROGRAM AND FRAMEWORK

i. **Global Privacy Policy**

1. This Policy identifies C-Path's approach to applying and demonstrating compliance with the privacy principles and applicable laws. The Policy is made available to all employees and is reviewed at planned intervals, at least annually, and:

a. whenever there is a material change in C-Path business practices that may impact the processing of personal data; and/or

b. whenever a monitoring activity (both a first-party audit and/or a second or third-party audit) highlights non-conformities to be corrected or areas that, even when compliant with applicable laws, can be improved; and/or

c. following an incident, breach, and/or complaint that highlights an area for improvement in the program

2. This Policy is supported by topic-specific policies, procedures, and standards that further describe the implementation of data privacy.

3. Because the varying activities undertaken by the business units may give rise to different types of privacy risks, specific implementations of these requirements may vary between business units/departments, though any such variation in implementation remains consistent with this Policy. The Company's policy is that new implementations have privacy by design and default.

4. Any personal data processing activity not consistent with this Policy must be submitted to the DPO for review and approval prior to undertaking such activity.

ii. **Contact:** Questions about this Policy should be directed to the Privacy Team at dpo@c-path.org.

iii. **Factors Influencing Privacy Management**

1. The following factors guide the privacy program and related policies:

a. legal and regulatory requirements

b. contractual factors such as agreements between C-Path and its vendors or contributor/members

c. business factors determined by a specific business application or in a specific use case

d. other factors that can affect the processing of personal data and associated privacy safeguarding requirements

iv. **Compliance with Legislation**

1. C-Path has identified and documented privacy legislation applicable to the Company in order to meet the requirements for the types of business, considering compliance in all relevant countries. Additional legislative requirements are identified (to the extent applicable) prior to beginning a new processing activity or operating in a new jurisdiction.

2. C-Path's DPO monitors the regulatory/legal environment to identify new regulatory/legal requirements. Once identified, the Privacy Team plans the necessary actions and changes to be

implemented to keep the framework and program compliant with the applicable requirements.

v. **Data Privacy Risk Assessment Process**

1. C-Path applies a privacy risk assessment process to identify potential risks of harm to data subjects, including risks to the privacy, rights, or freedoms of individuals which may result from personal data processing. Risks are assessed based on the likelihood of occurrence and seriousness of harm, and other potential consequences of the processing activity.
2. Identified risks are prioritized for risk treatment, which includes selecting risk treatment options and determining controls necessary to implement the risk treatment.
3. Risks to the confidentiality, integrity, and availability of personal data processing systems are evaluated and managed by the CTO and the Information Security team, in accordance with the Information Security Policy.

vi. **Data Protection Impact Assessment (DPIA)**

1. When new processing of personal data or changes to existing processing of personal data are planned, C-Path will identify and evaluate potential privacy impacts and identify required privacy controls necessary for such processing.
2. Considering the sensitivity of data, risk level of the processing activity, and relevant regulations, C-Path will also determine if there is a need to conduct a Data Protection Impact Assessment (DPIA) (sometimes also referred to as a Privacy Impact Assessment). A DPIA should be conducted for high-risk processing activities and must be conducted where mandated by relevant laws (see DPIA Policy for guidelines for when a DPIA is required).
3. A DPIA will include:
    a. A description of the processing activities, including types of data processed
    b. An assessment of the necessity and proportionality of the processing
    c. An assessment of the risks to the rights and freedoms of data subjects
    d. The measures envisaged to address the risk, including controls, safeguard, security measures and mechanisms to ensure the privacy and protection of personal data
    e. An overall assessment of the above elements to determine the necessity of consulting the relevant supervisory authority prior to the start of processing, as may be required by applicable law

vii. **Privacy by Design and Default**

1. C-Path promotes the philosophy of privacy by design and default. Processes and systems should be designed such that:
    a. the collection of personal data is limited to the minimum that is relevant, proportional and necessary for the identified purposes, and
    b. the processing (including use, disclosure, retention, transmission, and disposal) is limited to that which is adequate, relevant and necessary for the identified purposes
2. The design of any system that involves the processing of personal data must be preceded by an identification of relevant privacy control requirements. The privacy implications of new or substantially modified systems involving the processing of personal data should be resolved before those systems are implemented.

viii. **Monitoring, Review, and Audit**

1. **Monitoring:** C-Path will regularly evaluate the effectiveness of the privacy management program to ensure the necessary policies and controls are in place and whether controls comply with relevant data privacy regulations. C-Path will document results from monitoring.
2. **Management Review:** Management will periodically review the Company's privacy management program, including results of monitoring, to ensure its continuing suitability, adequacy, and effectiveness.
3. **Internal Audit**
    a. Management may initiate independent reviews of the privacy program to provide information on whether privacy systems and processes conform to the Company's requirements. Such reviews may be carried out by individuals independent of the area under review, such as the internal audit function, an independent manager or an external party organization specializing in such reviews.
    b. The independent review may be necessary to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing data privacy and should include assessing opportunities for improvement and the need for changes to the approach to privacy.
    c. The results of the independent review will be reported to Management. If the independent review identifies that the organization's approach and implementation to managing data privacy is inadequate, management will consider corrective actions.

ix. **Records Relating to Personal Data Processing (Processing Register) or Records of Processing Activity (ROPA):** C-Path will maintain records of the processing of personal data, including an

inventory or list of the personal data processing activities the Company performs. Such records will generally include the type of personal data, purpose of processing, categories of data, categories of data subjects, categories of recipients, and any other information which may be required by applicable law.

x. **Controller and Processor Relationships**

1. C-Path may act as a controller or processor depending on the specific processing activity.
2. When dealing with contributor/members, generally the contributor/member is the controller, and C-Path may be either a processor, a joint controller, or a separate controller.
3. Where C-Path enters a joint controller relationship, C-Path must determine and document the respective roles and responsibilities for compliance with data privacy laws and for the processing of personal data (including data protection and security requirements).

xi. **Obligations to Contributors/Members**

1. Where C-Path processes personal data on behalf of a contributor/member, in order to carry out a contributor/member engagement or provide a contributor/member service, the following applies:
    a. C-Path must provide the contributor/member with the appropriate information such that the customer can demonstrate compliance with their obligations.
    b. Personal data processed on behalf of a contributor/member must only be processed for the purposes in the agreement or compatible purposes, or on other documented instructions of the contributor/member.
    c. C-Path cannot use personal data processed under a contributor/member contract for the purposes of marketing and advertising, unless otherwise agreed.
    d. C-Path must inform the contributor/member if, in its opinion, a processing instruction infringes upon applicable legislation and/or regulation.
    e. C-Path may only engage a sub-processor to process personal data if and as permitted by the contributor/member contract.
    f. C-Path may only transfer personal data between jurisdictions if and as permitted by the contributor/member contract.
    g. If C-Path receives any legally binding requests for disclosure of personal data, C-Path must, after consulting with the Legal Department, notify the contributor/member of such request.

xii. **Employee Privacy:** C-Path respects the privacy of our employees. We will collect and handle personal employee data only for business reasons consistent with applicable laws. Access to personal employee data is limited only to those who have a need-to-know for the performance of their job, and in accordance with legal requirements. Those who are responsible for personal data are advised on a regular basis of their duty to protect this information. No one is permitted to access prospective, current or former employee records without proper authority. See the Employee Privacy Notice for further information.

7. DATA PRIVACY PRINCIPLES

a. C-Path and its employees must adhere to the following principles when processing personal data:

i. **Fairness and lawfulness:** there must be a legal ground that permits C-Path to process personal data. Where required by law, C-Path must obtain consent prior to collection, use, or disclosure of personal data.

ii. **Transparency:** C-Path must identify the purposes for which the personal data is being collected by C-Path at or before the time of collection and make information about its data privacy policies and practices publicly and readily available.

iii. **Purpose limitation:** data must be collected for specified, explicit and legitimate purposes, and may not be collected for one purpose and used for another, incompatible purpose (unless required by law or with the individual's consent).

iv. **Data minimization:** C-Path should only process personal data to the extent that is adequate, relevant, and limited to what is necessary for the purpose and not more.

v. **Accuracy:** personal data maintained by C-Path must be correct and kept up to date.

vi. **Storage Limitation:** Personal data must only be kept as long as required to serve the purposes for which it was collected. Once personal data is no longer needed for those purposes, it should be destroyed.

vii. **Security:** personal data must be kept secure using technical and organizational means appropriate to the sensitivity of information, to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage.

viii. **Individual Rights:** any processing activity must respect the rights of individuals and provide for specific data subject rights as required in certain jurisdictions.

ix. **Accountability:** C-Path is responsible for personal data under its control and is responsible for, and able to demonstrate compliance with, these principles.

8. PROCESSING OF PERSONAL DATA

a. Collection of Personal Data

i. Prior to collection, C-Path must identify and document the specific purposes for which the personal data will be processed and the relevant lawful basis for the processing for the identified purposes. Lawful grounds for processing personal data generally include:

1. When necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract
2. When necessary for compliance with a legal obligation to which C-Path is subject
3. When necessary for the purposes of legitimate interests of C-Path, including but not limited to: conducting business activities, internal administrative purposes, ensuring network and information security
4. Consent of the data subject, when consent is freely given, specific, informed, and an unambiguous indication of the data subject's wishes. Data subjects must be given the right to withdraw consent at any time.
5. Where laws and regulations otherwise permit processing collection of personal data must be limited to the minimum that is relevant, proportional, and necessary for the identified purposes.

b. Processing of Personal Data

i. Processing of personal data must be limited to that which is adequate, relevant, and necessary for the purposes identified prior to collection, unless a different purpose is required by applicable law or agreed to by the data subject. Use of personal data must be limited to that which is necessary in order to fulfil specific, explicit and legitimate purposes, and not processed for other incompatible purposes.

ii. Wherever possible, C-Path will use processing options which do not involve the identification of the individual data subject.

iii. C-Path should either delete personal data or render it in a form which does not permit identification or re-identification of data subjects, as soon as the original data is no longer necessary for the identified purpose(s). C-Path should ensure that personal data is as accurate, complete and up to date as is necessary for the purposes for which it is processed.

c. **Sharing/Disclosure of Personal Data:** Personal data must be treated as confidential, in accordance with the Records and Information Management Policy. C-Path must limit the disclosure of personal data to that which is necessary in order to fulfil specific purposes and minimize the number of people to whom personal data is disclosed or who are permitted to process it.

i. **Internal Company Disclosure:** Disclosure of personal data to Company employees is permitted on a legitimate business need-to-know basis, where necessary for the conduct of one's official duties.

ii. **Third Party Processors (Contractors, Vendors, Suppliers, Service Providers):**

1. C-Path may need to disclose personal data to a third-party processor to perform processing activities on behalf of C-Path. C-Path must have a written contract with any third-party processor, which requires that the processor:
    a. Has appropriate technical and organizational controls for privacy and security of personal data
    b. Only processes or discloses personal data for the purposes approved by C-Path
    c. Treats C-Path personal data as confidential
    d. Will report a personal data breach to C-Path without undue delay
    e. Complies with relevant data privacy laws and regulations
    f. Commits to provide information to C-Path and/or permit audits as necessary for compliance with privacy laws
2. Third Party processor contracts should also address the following, where relevant and in accordance with applicable laws or a Data Processing Addendum (DPA) should be executed:
    a. use of sub processors
    b. international transfers
    c. assistance to C-Path with meeting certain privacy obligations, such as responding to data subject access requests
    d. return or deletion of data at the end of the contract

iii. **Other Third-Party Disclosures**

1. Personal data should not otherwise be shared or disclosed outside of C-Path unless such disclosure is necessary for the performance of job duties, required by law, or where authorized to do so by the contributor/member or Information Owner in writing. The data subject must provide consent (or be given the ability to opt out, depending on jurisdiction) if the Company would like to sell personal data or disclose data for a purpose different from that for which it was collected.
2. Where external disclosure is permitted, a non-disclosure, confidentiality or other agreement may be required prior to such disclosure. Contact the Legal Department for guidance.
3. C-Path should record disclosures of personal data to third parties, including what has been disclosed, to whom and when.

d. Transmission of Personal Data

i. Personal data transmitted over a data transmission network (internet) must be subject to appropriate controls designed to ensure secure transfer and that the data reaches its intended destination.

ii. Personal data should be encrypted during transmission, where feasible, and sensitive personal data must be encrypted during transmission, whether to internal or external recipients.

e. Storage, Retention and Deletion

i. The Company will not retain personal data for longer than is necessary for the purposes for which the personal data is processed.

ii. The Company has adopted policies, procedures, and a retention schedule for personal data to retain data for a reasonable period, is necessary for the purpose of processing,

iii. After the retention period, personal data must be securely disposed of or fully anonymized. The Company has adopted policies and procedures for the secure disposal of personal data, as set forth in the Information Security Policy.

f. Cross Border Transfers

i. Laws of many jurisdictions prohibit or restrict cross border transfers of personal data. C-Path must comply with all laws restricting transfers as well as with any contractual obligations with contributor/members which may further restrict C-Path's ability to transfer data. C-Path documents the countries or regions to which personal data can be transferred pursuant to regulatory requirements, and the relevant legal basis for transfers between jurisdictions, where applicable.

ii. For example, GDPR restricts data transfers from the EU to countries outside the EU. C-Path may only transfer personal data from the EU to locations outside the EU where:

1. such countries provide for an adequate level of personal data protection as determined by the EU Commission
2. pursuant to contract terms or model clause agreements ensuring adequate data protection
3. as otherwise permitted under GDPR

iii. Laws of other jurisdictions where C-Path conducts business have similar requirements for cross-border transfers.

g. Notice and Transparency

i. Where C-Path is a data controller, C-Path has an obligation to ensure that data subjects are provided with appropriate information about the processing of their data (notice).

ii. C-Path will determine the legal, regulatory and/or business requirements for the type of information to be provided in the notice and the time at which to provide it. The notice must contain information identifying the data controller and describing the processing of personal data, as well as other information as required by applicable law.

iii. Information must be provided to data subjects in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience. Where

feasible, the information should be provided at the time of personal data collection.

h. Data Subject Rights

i. Under certain data privacy laws, data subjects may be entitled to some or all of the individual rights listed below. C-Path has adopted policies and procedures for handling requests from data subjects exercising the following data subject rights:

1. to obtain confirmation of whether personal data is being processed by C-Path
2. to obtain access to the personal data or obtain a copy of the personal data being processed
3. to ask C-Path to correct or amend personal data where it is inaccurate (rectification)
4. to ask C-Path to delete personal data
5. to object to C-Path processing data
6. to ask C-Path to restrict processing
7. the right to data portability
8. where processing is based on consent, the right to withdraw consent
9. rights in relation to automated decision making and profiling, including to request human intervention or challenge a decision
10. the right to challenge compliance or file a complaint with C-Path related to privacy

ii. C-Path will facilitate all data subject requests where required by law. C-Path will otherwise endeavor to facilitate all reasonable requests from data subjects, taking into account the nature of the processing and the extent technically feasible, and where doing so does not create undue burden for the Company.

iii. Requests by individuals to exercise their individual rights or submit a complaint must be handled by the Privacy Team and the DPO where applicable. C-Path will respond to data subject requests without undue delay, generally within one month, and in any case within the regulatory time limit. If C-Path determines that a data subject request cannot be facilitated, C-Path will provide the data subject with an explanation of why it has made that determination and a contact point for any further inquiries.

iv. Where required by applicable law, C-Path will inform third parties with whom personal data has been shared of any modification, withdrawal or objections pertaining to the shared data.

v. **If a C-Path employee receives any communication that could be considered a data subject request, they must notify the DPO immediately.**

9. PERSONAL DATA BREACH AND INCIDENT MANAGEMENT

a. The Company has adopted policies, procedures, and controls reasonably designed for a quick, effective, and orderly response to a personal data breach that enable the Company to meet its legal, regulatory, and contractual agreements with respect to personal data breaches.

b. Personal data breach events or suspected events must be immediately reported and handled in accordance with the Information Security Incident Response Plan (IRP). C-Path may be required to report a personal data breach to the relevant supervisory authority without undue delay and, in many jurisdictions, within 72 hours after becoming aware of it. C-Path may also be required to report the breach to affected data subjects or contributor/members. C-Path has established responsibilities and procedures for the notification to required parties, as set forth in the IRP.

c. Only the DPO and Legal Counsel are responsible for identifying the need and then notifying the supervisory authority.

10. COMPLIANCE

Any instance of non-compliance with this Policy must be reported immediately to the Information Security team, Privacy Team, or DPO. Any observed or suspected security weaknesses in systems or processes should also be reported. Violations of this Policy or applicable laws may result in corrective or adverse action, up to and including termination of employment or other appropriate action, and/or severe civil and criminal penalties and personal liability or criminal prosecution. C-Path reserves the right to change this Policy at any time. The revised Policy will be posted on the C-Path intranet and the "effective date" of this Policy will be updated accordingly. Employees are required to adhere to all aspects of this policy to the extent not otherwise prohibited by applicable local law.

11. REFERENCES

a. ISO/IEC 27001:2022 Information security management systems — Requirements
b. ISO/IEC 27002:2022 Information security controls
c. General Data Protection Regulation (GDPR)
d. California Consumer Privacy Act (CCPA)
e. Health Insurance Portability and Accountability Act (HIPAA)
f. NIST Privacy Framework
g. Information Security Policy
h. Information Security Incident Response Plan
i. Employee Privacy Notice

12. CHANGE LOG

Revision	Description of Changes	Author	Date
1.0	Initial Release	David Ross	06/14/22
1.5	Annual Update	David Ross	01/06/23
1.5	Annual Review	David Ross	06/04/23
1.5	Annual Review	David Ross	01/05/24
2.0	Reformatted to conform to the C-Path template. Expanded	Carlos Munoz	08/14/24

	references section, added mapping to legal and regulatory standards, added approvals section for signatures.		
2.1	Update to most recent policy template Aligned CTO role with existing policies	Carlos Munoz	09/02/25

13. MAPPING TO STANDARDS

Policy Section	ISO/IEC Standards	AI Laws and Regulations	US, State, and Global Privacy Laws and Regulations	U.S. CFR Reference	NIST Standards
1. Purpose, 2. Scope	ISO/IEC 27001:2022 Clause 4.1–4.3	N/A	GDPR (Art. 1–3), CCPA Sec. 1798.100–1798.199, HIPAA Privacy Rule 45 CFR §164	45 CFR §164 (HIPAA)	NIST Privacy Framework: ID.AM-1, ID.AM-5
3. Definitions	ISO/IEC 27000:2022 Terminology	ISO/IEC 42001:2023 Clause 3 (terms, if AI applies)	GDPR Art. 4, CCPA Sec. 1798.140	N/A	NIST Privacy Framework: ID.DE-1
4. Roles and Responsibilities	ISO/IEC 27001:2022 Clause 5.3, A.6.1.1–A.6.1.2	N/A	GDPR Art. 37–39 (DPO), CCPA enforcement obligations	N/A	NIST Privacy Framework: GV.RM-1, GV.PO-1
5. Reviews and Approvals	ISO/IEC 27001:2022 Clause 7.5, 9.3, 10.1	N/A	General privacy accountability principles	N/A	NIST Privacy Framework: GV.PO-2, GV.PO-3
6. Privacy Program and Framework	ISO/IEC 27701:2019 Clauses 5.4, 6.2; ISO/IEC 27001:2022 Clauses 6–10	ISO/IEC 42001:2023 Cl. 5.3, 6.3.2 (if AI involves personal data)	GDPR Rec. 78, Art. 5–6; CPRA Art. 1798.100(b), 1798.110, 1798.115	16 CFR Part 314 (GLBA Safeguards Rule)	NIST Privacy Framework: ID.GV-3, ID.IM-3, CM.AW-1

Policy Section	ISO/IEC Standards	AI Laws and Regulations	US, State, and Global Privacy Laws and Regulations	U.S. CFR Reference	NIST Standards
7. Data Privacy Principles	ISO/IEC 27001:2022 Annex A.5.1.1–A.5.1.2	OECD AI Principles (for fairness, transparency if AI applies)	GDPR Art. 5, CCPA Sec. 1798.100(b), Brazil LGPD Art. 6	N/A	NIST Privacy Framework: CT.PO-1, CT.PO-3, GV.PO-1
8. Processing of Personal Data	ISO/IEC 27001:2022 A.8, A.9, A.10, ISO/IEC 27701:2019 Clauses 7.2–7.4	ISO/IEC 42001:2023 Clause 8 (data quality & governance, if AI involved)	GDPR Art. 6–7, 12–14, 15–21; HIPAA; CPRA, and other state laws	45 CFR §164.502–514 (HIPAA)	NIST Privacy Framework: ID.CM-1, ID.CM-6, PR.DS-1–5
9. Personal Data Breach and Incident Management	ISO/IEC 27001:2022 Clause 6.1.3.d, A.5.25, A.5.29, ISO/IEC 27035-1:2016	N/A	GDPR Art. 33–34; CCPA Sec. 1798.150; HIPAA Breach Rule 45 CFR §§164.400–414	45 CFR §164.400–414 (HIPAA)	NIST SP 800-61; NIST Privacy Framework: RS.RP-1–5, RS.CO-1–5
10. Compliance	ISO/IEC 27001:2022 Clause 10	N/A	GDPR Art. 58, enforcement mechanisms; FTC Act §5	16 CFR Part 314; 15 U.S. Code §45	NIST Privacy Framework: GV.MT-1, GV.PO-3, DE.DP-1

14. APPROVALS

Name	Title	Signature	Date
Klaus Romero	Chief Executive Officer	Signed by: Klaus Romero	9/22/2025 | 3:52 PM MST
Kristen Swingle	President & Chief Operating Officer	Signed by: Kristen L. Swingle	9/22/2025 | 3:57 PM MST
Richard Liwski	Chief Technology Officer	Signed by: Richard Liwski	9/24/2025 | 1:32 PM MST
David Ross	Data Protection Officer	Signed by: David Ross	9/23/2025 | 3:37 AM MST
Carlos Munoz	ISMS Manager	Signed by: Carlos Munoz	9/22/2025 | 3:50 PM MST