KNOW YOUR CUSTOMER (KYC) POLICY

Ontoly Building Emissions Reduction Standard — BERS Program

Version 1.1 — August 24, 2026

1483124 BC Ltd. dba Ontoly

1. Purpose, Authority and Regulatory Status

1.1 Purpose. This Know Your Customer (KYC) Policy establishes procedures to verify the identity of Account Holders, to prevent the BERS Program from being used to launder money, finance terrorism or evade sanctions, and to protect the integrity and credibility of BERUs and the Ontoly Registry.

1.2 Authority. Authority for this Policy is derived from BERS Standard, Section 2.6 (Financial Controls) and Section 5.2.3 (Verification Requirements), and from Ontoly's responsibility as administrator of a carbon crediting program to maintain institutional integrity. This Policy is one of the Ontoly Program Rules and is binding on all Ontoly personnel.

1.3 Regulatory status — reporting entity assessment. Ontoly has assessed whether it is a "reporting entity" under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 (Canada) ("**PCMLTFA**") or a "financial institution" under the *Bank Secrecy Act*, 31 U.S.C. § 5311 et seq. (United States) ("**BSA**"). Based on its current activities, Ontoly does not fall within any prescribed reporting entity or financial institution category. In particular, Ontoly does not deal in foreign exchange, remit or transmit funds, issue or redeem money orders or other negotiable instruments, operate a marketplace, crowdfunding or payment platform, cash cheques, or provide virtual currency exchange services, and it is not a financial entity, securities dealer, casino, real estate professional or other prescribed sector. **The purchase price for BERUs is paid by the buyer directly to the Building Representative, away from the Ontoly Platform; as provided in Section 6B.3 of the Platform Terms, Ontoly does not receive, hold, escrow, control, disburse or have custody of any buyer or seller funds at any time, and provides no payment, settlement, remittance or escrow facility. The only money Ontoly collects is its own fees under Part XII of the Platform Terms, paid to Ontoly by the Person who owes them. Ontoly accordingly has no statutory obligation to register with FINTRAC or FinCEN, to file Suspicious Transaction Reports or Suspicious Activity Reports, or to maintain a statutory compliance program under the PCMLTFA or the BSA.**

1.4 Voluntary application. Notwithstanding Section 1.3, Ontoly applies the controls in this Policy as a matter of program governance, because financial-crime controls are essential to stakeholder confidence in the BERS Program and are aligned with ICVCM Criterion 1.1 (Credibility and Transparency) and with international good practice. These controls are contractual and governance measures, not statutory obligations, and they are calibrated to the size of Ontoly's operations and the risk profile of the BERS Program.

1.5 Obligations that apply regardless of reporting entity status. Sanctions compliance is **not** sector-specific. Every person and entity in Canada is prohibited from dealing with designated persons under the *Special Economic Measures Act*, the *United Nations Act*, the *Justice for Victims of Corrupt Foreign Officials Act* and the *Criminal Code*, and any person subject to US jurisdiction is likewise bound by sanctions administered by the Office of Foreign

Assets Control (OFAC). The sanctions screening, freezing and reporting obligations in Part 8 of this Policy are **mandatory legal obligations and are not discretionary**, and nothing in Section 1.3 or 1.4 reduces them.

1.6 Change in status. If Ontoly's activities change — in particular if Ontoly begins to receive, hold, escrow or disburse client funds, to process the purchase price payable between Account Holders, to exchange fiat currency for BERUs, to operate a settlement facility or a public marketplace, or to provide any service described in Section 1.3 — the Compliance Officer shall promptly reassess Ontoly's status and, where required, register with FINTRAC or FinCEN and implement a full statutory compliance program. This assessment shall be revisited at each annual review.

1.7 Review. This Policy is reviewed annually and updated to reflect evolving risks, regulatory guidance and operational experience.

2. Scope and Trigger Point

2.1 Trigger point. Customer due diligence under this Policy is completed **at the point a person requests an Ontoly Portal account**, and must be completed and approved **before the account is activated**. No Portal account is activated, and no Project may be listed, no BERU may be issued, transferred, sold, accepted or Retired, until due diligence is complete.

2.2 Public Registry access is not in scope. The Ontoly Registry is a public-facing database that may be viewed without an account. Ontoly does not collect identity documents from, or conduct due diligence on, members of the public who view the Registry.

2.3 Persons in scope. This Policy applies to all applicants for an Ontoly Portal account, including Building Owners, Building Representatives and their authorized agents (Supplier Accounts), and individual investors, aggregators, financial institutions and corporations acquiring or Retiring BERUs (Buyer Accounts).

2.4 Validation Bodies and Verification Bodies. Validation Bodies and Verification Bodies contracted by Ontoly for a Validation Cohort or a Verification Cohort are subject to entity-level verification, accreditation confirmation and beneficial ownership identification under this Policy. Their individual personnel are subject to identity confirmation only, and are not subject to beneficial ownership, PEP or source-of-funds review, unless they hold an Ontoly Portal account in their own right.

2.5 Counterparties. Counterparties to BERU transactions conducted through the Ontoly Portal are in scope by virtue of being required to hold an Ontoly Portal account. Ontoly does not conduct due diligence on transactions occurring entirely outside the Ontoly Platform.

2.6 Buyers. Every buyer of BERUs must hold an activated Ontoly Portal account and must complete customer due diligence under Parts 4 to 7 of this Policy before any BERU is transferred to it. Consistent with Section 6B.7 of the Platform Terms, there is no guest, unregistered or anonymous route by which a BERU may be acquired, held or Retired, and no purchase of BERUs is available without an account. Sanctions screening under Part 8 applies to every buyer and to every transfer. Purchases are available only from the Eligible Jurisdictions published on the Ontoly Portal, in accordance with Section 6B.15 of the Platform Terms.

2.7 Jurisdiction. This Policy applies to BERS Program activities wherever they are conducted. Where an applicant, a Beneficial Owner, a controlling person or a Project is located in a jurisdiction other than Canada or the United States, any additional identity verification, customer due diligence, sanctions, reporting or record-keeping requirement applicable in that jurisdiction supplements rather than replaces this Policy, and the Compliance Officer shall determine what additional measures apply before an account is activated. Ontoly may decline to open an account where it is unable to satisfy an applicable local requirement.

3. Definitions

3.1 Beneficial Owner. The natural person or persons who ultimately own or control a legal entity, being any natural person who directly or indirectly owns or controls 25% or more of the voting interests or equity. Where no natural person meets that threshold, the Beneficial Owner is the natural person exercising effective control (for example, Chief Executive Officer, Managing Director or Board Chair).

3.2 CDD (Customer Due Diligence). Identification and verification of the identity and beneficial ownership of an applicant, together with ongoing monitoring proportionate to risk.

3.3 EDD (Enhanced Due Diligence). Heightened measures applied to Higher Risk customers, including source of funds verification, enhanced beneficial ownership scrutiny and senior approval.

3.4 PEP (Politically Exposed Person). An individual who holds or has held, within the past five (5) years, a prominent public position, together with their immediate family members and known close associates, as further defined in Part 7.

3.5 Sanctions List. Government-maintained lists of designated persons and entities, including the OFAC Specially Designated Nationals (SDN) and consolidated lists (United States), Canada's Consolidated Autonomous Sanctions List (Global Affairs Canada), and the United Nations Security Council consolidated lists.

3.6 Escalation Report. An internal record prepared under Part 10 documenting a suspicious indicator, its assessment and the action taken. An Escalation Report is an internal governance document and is not a Suspicious Transaction Report or Suspicious Activity Report.

4. Customer Identification Program

4.1 Individual applicants — electronic verification is the primary method. Ontoly shall verify the identity of each individual applicant using a dedicated electronic identity verification provider, which confirms the applicant's name, date of birth and residential address against independent data sources. **Where electronic verification returns a confirmed match, no identity document is required and none shall be requested.**

4.2 Individual applicants — when an identity document is requested. Ontoly shall request a current, unexpired government-issued photo identification document (passport, driver's licence or national identity card) **only where**: (a) electronic verification under Section 4.1 is inconclusive or returns a partial match that cannot otherwise be resolved; (b) a discrepancy in the information provided cannot be resolved from other sources; or (c) the applicant is classified as Higher Risk under Part 6. Where a document is requested it shall be verified against an independent source. Sole reliance on a self-submitted image, without independent verification, is not acceptable.

4.3 What is recorded from an identity document. Where an applicant provides a government-issued photo identification document, Ontoly shall record the document type, issuing authority, document number, expiry date and the outcome of verification. Ontoly shall not retain an image or copy of the document after verification is complete.

4.4 Individual applicants — address. Where the electronic verification performed under Section 4.1 confirms the applicant's residential address, no address document is required. Where it does not, Ontoly shall obtain a document confirming the applicant's residential address, such as a utility bill, bank statement or lease agreement, dated within six (6) months prior to application.

4.5 Entity applicants — legal status. Ontoly shall confirm the entity's current registration and good standing against the applicable corporate registry. Where registry confirmation is unavailable or inconclusive, Ontoly shall obtain the entity's certificate of incorporation, articles of organization or equivalent constating documents. Copies are sufficient; notarized or certified copies are not required.

4.6 Entity applicants — ownership and control. Ontoly shall obtain a beneficial ownership declaration signed by an authorized officer identifying all Beneficial Owners and all directors and officers with decision-making authority, and a current business licence or registration where applicable. An organizational chart is required only where the ownership structure includes more than one intermediary layer.

4.7 Verification methods. Ontoly shall not obtain consumer credit reports for identity verification purposes, in order to avoid engaging obligations under the US *Fair Credit Reporting Act* and comparable Canadian credit reporting legislation. Ontoly does not use facial recognition, liveness detection or any other biometric identification technology, and does not create, collect or store biometric identifiers or templates. Where a documentary discrepancy cannot be resolved electronically, Ontoly may request a supplementary document or arrange a live video call for the sole purpose of confirming that the person presenting a document is the person shown in it; no recording is retained beyond confirmation of the outcome, and no biometric template is generated.

4.8 Data minimization. Ontoly shall collect the minimum information necessary to verify identity and to assess financial-crime risk, and shall not request documentation that is not required by this Policy. Ontoly's handling of the information collected under this Part is governed by the Ontoly Privacy Statement.

4.9 Currency of documentation. Information and any supporting documentation shall be current and, in the case of a document, unexpired at the time of submission. Ontoly shall request refreshed information at the periodic review intervals in Part 9, or where a document material to verification has expired.

5. Beneficial Ownership Determination

5.1 Threshold. Ontoly shall identify each natural person who owns or controls, directly or indirectly, 25% or more of the voting equity or decision-making authority of an entity applicant. Each such person shall be identified and verified in accordance with Part 4.

5.2 Controlling person. Where no natural person meets the 25% threshold, Ontoly shall identify and verify the natural person exercising effective control over the entity's operations, strategic decisions or financial matters.

5.3 Layered structures. Where an entity applicant is owned through intermediary entities, Ontoly shall trace ownership to the natural person level. Where tracing is obstructed or cannot be completed, the applicant shall be classified as Higher Risk under Part 6 or refused under Part 11.

5.4 Trusts and similar structures. For a trust or comparable structure, Ontoly shall identify and verify: (a) the settlor; (b) the trustee or trustees; and (c) any beneficiary entitled to 25% or more of the trust's capital or income. **Ontoly does not require identification of contingent or discretionary beneficiaries holding less than a 25% entitlement**, unless the trust is classified as Higher Risk, in which case the full beneficiary class shall be identified. Ontoly shall also identify any natural person holding power to amend or revoke the trust.

5.5 Documentation. The applicant shall provide a signed Beneficial Ownership Declaration confirming the accuracy and completeness of the information provided. Ontoly shall verify the declaration against corporate registry records and, where the entity is Higher Risk, against at least one additional independent source.

6. Risk-Based Due Diligence

6.1 Two-tier framework. Ontoly classifies each customer as either **Standard Risk** or **Higher Risk**. Applicants are Standard Risk by default. An applicant is Higher Risk where one or more of the factors in Section 6.4 is present.

6.2 Standard Risk — measures. Electronic identity verification under Part 4, beneficial ownership identification under Part 5, sanctions and PEP screening under Parts 7 and 8, and a declaration of the source of funds used to pay Ontoly fees or to acquire BERUs. Periodic review every three (3) years, plus event-driven review under Part 9.

6.3 Higher Risk — measures. All Standard Risk measures, plus: (a) a government-issued photo identification document for each individual concerned, verified in accordance with Section 4.2; (b) documentary verification of source of funds through bank statements, financial statements, tax documentation or comparable primary sources; (c) adverse media and litigation screening; (d) confirmation of business legitimacy against an independent source; (e) written approval of account opening by the Compliance Officer; and (f) periodic review annually. Transaction limits or pre-approval requirements may be imposed until risk is mitigated.

6.4 Higher Risk factors. An applicant is Higher Risk where: (a) the applicant, a Beneficial Owner or a controlling person is a PEP within Part 7; (b) a sanctions screening match is unresolved; (c) beneficial ownership is opaque, obstructed or involves bearer instruments; (d) the applicant, a Beneficial Owner or a controlling person is resident or incorporated in, or the Project is located in, a jurisdiction on the FATF list of high-risk or increased-monitoring jurisdictions; (e) adverse media, regulatory findings or criminal charges relevant to financial crime, fraud or environmental misrepresentation are identified; (f) the applicant declines or fails to provide information required under this Policy; or (g) the Compliance Officer determines on documented reasons that elevated risk is present.

6.5 Proportionality. Ontoly shall apply this Part proportionately. Where an applicant is a publicly listed company, a government or public body, a regulated financial institution, or a wholly-owned subsidiary of any of them, Ontoly may rely on that status in place of full beneficial ownership tracing, and shall record the basis for doing so.

7. Politically Exposed Persons

7.1 Screening. Ontoly shall screen all applicants, Beneficial Owners and controlling persons against PEP data at account opening and at each periodic review under Part 9, using a commercially available screening provider. Positive matches shall be escalated to the Compliance Officer.

7.2 Definition. For the purposes of this Policy, a PEP is an individual who holds, or has held within the past five (5) years: head of state or government; a senior government, ministerial or deputy-ministerial position; a senior judicial office; a senior military rank; a senior executive position in a state-owned enterprise; or a senior decision-making position in an international organization.

7.3 Family members and close associates. PEP status extends to the **spouse or common-law partner, children and parents** of a PEP, and to any person publicly known to be closely associated with a PEP in a business or financial capacity. **Siblings, grandchildren and more remote relatives are not within scope** unless screening or adverse media independently indicates a relevant connection.

7.4 Consequence of PEP status. A PEP, or an immediate family member or close associate of a PEP, is classified as Higher Risk and is subject to EDD under Section 6.3. Account opening requires written approval by the Compliance Officer. CEO approval is required only where the PEP holds or held a position described in Section 7.2 within the preceding twelve (12) months. Where a PEP's public service ended more than five (5) years ago and no other Higher Risk factor is present, the Compliance Officer may reclassify the customer as Standard Risk on documented reasons.

8. Sanctions Screening — Mandatory

8.1 Legal character. The obligations in this Part are mandatory legal obligations applicable to Ontoly irrespective of its status under Section 1.3. They may not be waived, deferred or applied on a risk-sensitive basis.

8.2 Screening. Ontoly shall screen every applicant, Beneficial Owner, controlling person and transaction counterparty against the Sanctions Lists: (a) before account activation; (b) before each BERU issuance, transfer, acceptance or Retirement, and before Ontoly records the transfer of any BERU acquired through the Ontoly Portal; (c) upon any change to customer identity or beneficial ownership information, within five (5) Business Days; and (d) whenever a relevant Sanctions List is updated, by means of an automated ongoing monitoring service applied to the existing customer base.

8.3 Event-driven rather than calendar-based. Screening under Section 8.2 is triggered by events and by list updates rather than by a fixed quarterly cycle. Where Ontoly's screening provider does not offer continuous list-update monitoring, Ontoly shall conduct a full portfolio rescreen no less frequently than every six (6) months.

8.4 Positive match. On a confirmed match, Ontoly shall immediately: (a) freeze the account and all BERUs held in it; (b) escalate to the Compliance Officer and CEO within 24 hours; (c) preserve all related records; (d) make any report or disclosure required by applicable sanctions law, including disclosure to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service under Canadian sanctions legislation and reporting of blocked property to OFAC within the period prescribed by US law; and (e) not process any transaction for the customer.

8.5 Partial and fuzzy matches. Where screening returns a partial or phonetic match, Ontoly shall conduct manual review within five (5) Business Days, comparing identifiers held on file against the listing. Pending resolution, the account shall be treated as matched and transactions shall not proceed. The outcome of every manual review shall be documented.

8.6 No dealings. Ontoly shall not permit any BERU transaction involving a confirmed designated person. Accounts with a confirmed match shall be closed and balances frozen pending direction from the competent authority.

9. Ongoing Monitoring

9.1 Periodic review. Ontoly shall review customer information and risk classification every three (3) years for Standard Risk customers and annually for Higher Risk customers. Review confirms that information remains current and that the risk classification remains appropriate.

9.2 Event-driven review. Ontoly shall conduct an immediate review on: (a) a change in beneficial ownership of 25% or more; (b) adverse media or regulatory findings relevant to financial crime, fraud or environmental misrepresentation; (c) a new PEP or sanctions match; (d) a material change in transaction pattern or volume; (e) discovery of material misrepresentation in account information; or (f) a Corrective Action Notice or enforcement finding under the BERS Standard.

9.3 Transaction monitoring. Ontoly shall monitor Platform Activities for patterns inconsistent with the customer's stated Account Purpose Declaration, including structuring of BERU purchases or transfers, rapid accumulation and immediate Retirement without a stated accounting purpose, transfers to or from higher-risk jurisdictions, and undisclosed third-party beneficiaries. Monitoring may be automated; automated alerts require human review before any action is taken.

9.4 Refresh. At each periodic or event-driven review, Ontoly shall obtain confirmation from the customer that previously provided information remains accurate, and shall obtain refreshed information or documentation only where information has changed or a document has expired. A full re-collection of documentation at every review is not required, and an identity document shall not be requested at review except in the circumstances set out in Section 4.2.

10. Escalation, Investigation and Cooperation with Authorities

10.1 No statutory suspicious transaction reporting obligation. As set out in Section 1.3, Ontoly is not currently a reporting entity under the PCMLTFA or a financial institution under the BSA, and therefore has no statutory obligation to file Suspicious Transaction Reports with FINTRAC or Suspicious Activity Reports with FinCEN. Ontoly shall not file such reports unless and until it becomes a reporting entity, both because the reporting channels are available to reporting entities and because disclosing customer personal information to a financial intelligence unit without lawful authority may itself contravene privacy legislation.

10.2 Internal escalation. Any Ontoly personnel who identify a suspicious indicator shall report it to the Compliance Officer within two (2) Business Days. The Compliance Officer shall assess the matter and prepare an Escalation Report within ten (10) Business Days, recording the indicator, the assessment, the evidence considered and the action taken.

10.3 Available actions. Following assessment the Compliance Officer may: (a) request further information or documentation from the customer; (b) reclassify the customer as Higher Risk and apply EDD; (c) impose transaction limits or suspend the account; (d) refuse or terminate the relationship under Part 11; (e) cancel or withhold BERUs in accordance with the Platform Terms; or (f) refer the matter to law enforcement under Section 10.4.

10.4 Voluntary referral to law enforcement. Where the Compliance Officer forms a reasonable belief that a criminal offence has occurred, Ontoly may refer the matter to the appropriate police force or regulator. Before making a voluntary referral that discloses personal information, the Compliance Officer shall confirm that the disclosure is permitted under applicable privacy legislation — including the provisions of PIPEDA and the BC *Personal Information Protection Act* that permit disclosure without consent for the purpose of investigating a breach of an agreement or a contravention of law — and shall document that assessment in the Escalation Report.

10.5 Mandatory disclosures preserved. Nothing in this Part limits: (a) the mandatory sanctions reporting obligations in Part 8; (b) Ontoly's obligation to respond to a subpoena, production order, search warrant or other lawful compulsion; or (c) any reporting obligation that arises if Ontoly becomes a reporting entity.

10.6 Confidentiality of investigations. Ontoly personnel shall not disclose to a customer, or to any person acting for a customer, the existence or substance of an ongoing investigation or referral where disclosure would prejudice the investigation, contravene a court order or non-disclosure requirement, or breach a legal obligation. This is a confidentiality requirement of this Policy. The statutory "tipping-off" offence under the PCMLTFA and the BSA does not apply to Ontoly while it is not a reporting entity, and personnel should not be advised that it does.

10.7 Records. Escalation Reports and supporting material shall be maintained separately from general customer files, with access restricted to the Compliance Officer, the CEO, external auditors and competent authorities.

11. Account Refusal and Termination

11.1 Grounds. Ontoly may refuse to open, or may suspend or terminate, an account where: (a) identity cannot be verified to Ontoly's satisfaction; (b) a confirmed sanctions match exists; (c) beneficial ownership cannot be established; (d) there are reasonable grounds to suspect money laundering, terrorist financing, sanctions evasion or fraud; (e) material misrepresentation or false documentation has been provided; or (f) a PEP or other Higher Risk relationship presents risk that Ontoly determines it cannot manage.

11.2 Suspension. On discovery of a breach of this Policy, Ontoly may suspend the account and freeze all BERUs held in it pending investigation, in accordance with Section 3.8 of the Platform Terms.

11.3 Reasons. Ontoly shall provide the customer with the general category of concern giving rise to a refusal, suspension or termination — for example, "identity could not be verified" or "required documentation was not provided" — except where doing so would prejudice an investigation, contravene sanctions law, or breach a legal obligation. Ontoly is not required to disclose the detail of its risk assessment methodology, screening criteria or investigative steps.

11.4 Appeal. A customer may request review of a refusal, suspension or termination within thirty (30) days by writing to the Compliance Officer. The Compliance Officer shall respond within thirty (30) days. Where the decision is upheld or no appeal is lodged, the account shall be closed and BERUs dealt with in accordance with the Platform Terms and applicable law.

12. Record Retention

12.1 CDD and EDD records. Records of identity verification and its outcome, the details recorded under Section 4.3, beneficial ownership declarations, address verification results, screening results and risk assessment records shall be retained for seven (7) years from the date of account closure. Images or copies of identity documents shall not be retained after verification is complete.

12.2 Transaction records. Records of BERU issuance, transfer, acceptance, Retirement and cancellation shall be retained for seven (7) years from the date of the transaction, and Registry entries shall be retained on the long-term basis described in the Ontoly Privacy Statement.

12.3 Escalation Reports. Escalation Reports and supporting material shall be retained for seven (7) years from the date of the report.

12.4 Accessibility and security. Records shall be maintained in secure digital form with role-based access control and shall be readily retrievable for audit or investigation. The Compliance Officer is custodian of all KYC records.

12.5 Disposal. Records shall be securely destroyed at the end of the applicable retention period unless a legal hold applies.

13. Training

13.1 Initial training. Personnel with customer-facing or compliance responsibilities shall complete AML, sanctions and KYC training at onboarding, covering this Policy, sanctions obligations, identity verification, beneficial ownership, escalation procedures and privacy obligations in handling customer information.

13.2 Refresher training. Covered personnel shall complete refresher training annually. Where Ontoly has fewer than ten (10) covered personnel, refresher training may be delivered as a documented briefing by the Compliance Officer rather than a formal course.

13.3 Records. Training attendance and completion records shall be retained for seven (7) years.

14. Compliance Officer

14.1 Designation. Ontoly shall designate a named individual as Compliance Officer, responsible for administering this Policy, including risk classification, screening, escalation, record retention and training. The Compliance Officer reports to the CEO and has direct access to the BERS Governance Board.

14.2 Annual review. The Compliance Officer shall conduct an annual review of the effectiveness of this Policy, including the reporting entity assessment under Section 1.6, the adequacy of screening, the quality of escalation handling and the appropriateness of risk classifications, and shall report the results to the BERS Governance Board.

14.3 Reporting. The Compliance Officer shall report annually to the BERS Governance Board on accounts opened, refused and terminated; the outcome of periodic reviews; sanctions and PEP matches; Escalation Reports and their disposition; regulatory developments; and recommended changes to this Policy.

15. Review and Amendment

15.1 Annual review. The Compliance Officer and the BERS Governance Board shall review this Policy annually, taking account of changes in financial-crime risk, regulatory guidance from FINTRAC, FinCEN, OFAC, Global Affairs Canada and provincial regulators, ICVCM requirements, and operational experience.

15.2 Amendment. Material amendments require approval by the CEO and shall be reported to the BERS Governance Board within thirty (30) days. Non-material clarifications may be made by the Compliance Officer with notice to the CEO. A thirty (30) day transition period applies to material amendments except where immediate implementation is required by law.

15.3 Relationship to other documents. This Policy is one of the Ontoly Program Rules and is to be read with the Ontoly Platform Terms and Conditions, the Ontoly Privacy Statement, the Ontoly Cookie Policy, the Acceptable Use Policy and the E-Sign Consent. Capitalized terms used but not defined in this Policy have the meanings given to them in the Platform Terms. Consistent with Section 2.4 of the Platform Terms, the Ontoly Privacy Statement governs the handling of personal information and this Policy governs the conduct of due diligence.