Relativity Terms and Conditions

Document Control	
Document ID	Relativity Terms & Conditions
Version	(S&B 1.3 v16.12.2025)
Classification	Commercial in confidence
Document Status	Final
Modified By	Stevens & Bolton
Document Date	16/12/2025
Owner	Greg Wildisen

RelativityOne Terms and Conditions

These Relativity Terms and Conditions (including, without limitation any and all Exhibits, attachments and addendums hereto, collectively, the "Master Terms"), apply between you ("you", "Client") and Conduent Business Process Solutions Limited (company number 04022569) ("Conduent").

1. DEFINITIONS

Access Credentials	Any username, password, license or security key, or other information used to verify an individual's identity and authorization to access and use the Software.
Affiliate	With respect to any entity, any other entity that directly or indirectly controls, is controlled by, or is under common control with such entity, where "control" (including "controlled by" and "common control") means the ability to, directly or indirectly, direct the management, operations or policies of such entity.
Relativity Agreement	Collectively, these Master Terms and any Orders.
Authorized User	Any person who accesses the Software using Access Credentials for or on behalf of Client. Authorized Users may include Representatives, Affiliates of Client, and their end users.
Claim	Claim, action, cause of action, demand, lawsuit, arbitration, inquiry, audit, notice of violation, proceeding, litigation, citation, summons, subpoena, or investigation of any nature, whether civil, criminal, administrative, regulatory, or other, whether at law, in equity or otherwise.
Confidential Information	Information, whether disclosed orally or in writing, that is identified by the disclosing party as confidential or that is of a nature that a reasonable person would suspect to be confidential or proprietary to the disclosing party or a third party, including data or information provided by Client to Conduent and any information relating to a party's business practices, products, product development, research, marketing plans, customer information, financial information, and pricing rates and methodologies. For purposes of clarity, Client's Confidential Information includes Client Data and Conduent's Confidential Information and Panoram's Confidential Information includes the Software and the terms of the Relativity Agreement and Panoram's Confidential Information includes the Panoram Agreement.
Client Data	All documents, files and other data that Client or its Authorized Users import into the Software and all work product results of all work that Client and its Authorized Users perform respecting such data in the Software. For clarity, Client Data does not include system and data usage metrics and billing information, Usage Data, or any systems' operations, performance or security information.
Data Security Terms	The Data Security Terms incorporated by reference into the Relativity Master Terms.
Derivative Works	Every translation, portation, modification, correction, addition, extension, upgrade, improvement, compilation, abridgment or other form in which an existing work may be recast, transformed or adapted, including any software, technology, methods or processes that a person skilled in the arts would consider to be derived from the existing work or

	from the existing work owner's technology, methods or processes protected by copyright, patent or trade secret laws.
Documentation	The documentation for the Software referenced in the applicable Scope of Work.
Harmful Code	Any software, hardware, or other technology, device, or means, including any virus, worm, malware, or other malicious computer code, the purpose or effect of which is to permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any: (a) computer, software, firmware, hardware, system, or network; or (b) application or function of any of the foregoing or the security, integrity, confidentiality, or use of any data processed thereby.
Intellectual Property Rights	Any and all rights arising from or under any of the following, whether protected, created or arising under the Laws of the United States of America or any other jurisdiction: patents (including any applications, extensions, divisions, continuations, continuations-in-part, re-examinations, reissues, and renewals related thereto), copyrights (including any applications, registrations and renewals related thereto), trademarks and service marks (including applications, registrations and renewals related thereto), trade dress, trade names, trade secret and know-how and any other intellectual property or proprietary rights of any nature, by whatever name or term known or however designated.
Laws	Statutes, laws, ordinances, regulations, rules, codes, orders, constitutions, treaties, common laws, judgments, decrees, or other requirements of any federal, state, local, or foreign government, including any of the foregoing respecting the security and privacy of personal data, anti-bribery and anti-corruption, anti-terrorism, non-discrimination and non-harassment, and export restrictions.
Losses	Losses, damages, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees.
Order	A Scope of Work to the Panoram Agreement pursuant to which Conduent shall provide Software or SaaS Product to Client and its Authorized Users, including (a) to the extent expressly referenced therein, any attachments thereto or documents incorporated therein, and (b) any amendments thereto.
Panoram	means Panoram Digital Limited (company number 12419388).
Panoram Agreement	the relevant Agreement between the Client and Panoram.
Representatives	(a) with respect to Panoram, Panoram's employees, officers, directors, consultants, agents, independent contractors, service providers, subcontractors, and legal advisors; (b) with respect to Conduent, Conduent's employees, officers, directors, consultants, agents, independent contractors, service providers, subcontractors, and legal advisors (c) with respect to Client, Client's employees, officers, directors, consultants, agents, independent contractors, service providers, subcontractors, and legal advisors; and (d) with respect to Affiliates, the Affiliate's employees, officers, directors, consultants,

	agents, independent contractors, service providers, subcontractors, and legal advisors.
SaaS Product	Relativity Software accessed and used as a software-as-a-service platform.
Software	All technology components incorporated in or made available in connection with a SaaS Product, and any other software products, along with any Documentation relating thereto and any know-how provided by Conduent in connection with the provision of the Software or related services designed to assist Client with the operation of the Software. For clarity, the term "Software" in any documents incorporated by reference into any Order refers only to the Software provided pursuant to that Order.

2. ACCESS TO AND USE OF THE SOFTWARE

2.1 Right to Access and Use the Software

Conduent hereby grants Client a worldwide, non-exclusive, non-transferable right of access to and use of the Software during the term of the applicable Order (as set forth in the applicable Order). The right granted in this Section 2.1 includes permission to import, process, review, use, copy, store, and transmit Client Data to, in and from the Software, subject to the terms of the Relativity Agreement and the Panoram Agreement.

2.2 Use of the Software by Authorized Users

Client may provide access to the Software to any of its Representatives to enable them to be Authorized Users. Access to and use of the Software by any Authorized User will be considered access to and use of the Software by Client for purposes of the Relativity Agreement and the Panoram Agreement. For purposes of clarity: (a) all Authorized Users' billable items will be aggregated with Client's billable items for purposes of determining fees due under the applicable Order; (b) Client will be responsible for payment of all fees due under the Relativity Agreement and the Panoram Agreement; (c) Client shall cause all Authorized Users to comply with the Relativity Agreement and the Panoram Agreement; and (d) Client will be responsible for the acts and omissions of each Authorized User, including any failure by any Authorized User to comply with the Relativity Agreement and/or and the Panoram Agreement, as though they were the acts and omissions of Client.

Client may not host or sub-host the Software, administer the Software or provide or enable any functions of the Software under any white label or private label re-hosting arrangement. If Conduent and/or Panoram notifies Client that Client has violated any of the foregoing restrictions, Client will take all steps reasonably necessary (working in cooperation with Conduent and/or Panoram) to remedy the violation.

2.3 Access Credentials

Client will require each Authorized User to have separate Access Credentials. Neither Client nor any Authorized User will share or repurpose Access Credentials, regardless of whether the sharing occurs at the same or different times. The username of each Authorized User must be a unique working email address. Client will be responsible for all access to and use of the Software utilizing Client Access Credentials. Client will promptly notify Conduent and Panoram of any known or reasonably suspected unauthorized use of any Access Credentials.

2.4 Services

Conduent will provide the services as set forth in the applicable Order ("Services"). Upon Client's request and at Conduent's discretion, Conduent may provide additional services relating to the Software and/or SaaS Product, pursuant to written documentation, between the parties and payment of Conduent's, and/or where applicable Panoram's, then-current hourly rates.

Client acknowledges that in connection with any services provided in connection with the Relativity Agreement (including Services) and/or the Panoram Agreement, neither Conduent or Panoram nor any Conduent or Panoram Representative is providing legal advice or interpretation of legal documents. Services provided by Conduent and/or Panoram and Conduent and/or Panoram Representatives are not intended to be, and should not be construed as, legal advice. Client is solely responsible for its use of the Software, including deciding whether, to what extent, and how to use particular features of the Software for any given use case.

2.5 Updates to the Software and Additional Products

Conduent may make changes to the Software at its discretion, including to enhance the quality, delivery or performance of the Software, and to provide corrections. The timing of any updates to a SaaS Product shall be at Conduent's discretion. Conduent will not make any changes to the Software during the term of the applicable order (as set forth in the applicable Order) that materially degrade the overall functionality of the Software, unless: (a) the changes are to comply with applicable Laws; (b) the changes are required to resolve a defect or security issue; or (c) Conduent provides a functional equivalent.

From time to time, Conduent and Panoram may make additional products available. At Conduent and Panoram's reasonable discretion, such additional products may be: (a) included with the Software at no additional charge, in which case such products are subject to the terms of the Panoram Agreement and the Relativity Agreement unless stated otherwise in the Documentation; or (b) made available for additional fees, in which case Client may choose to subscribe to such products by signing an additional Order.

2.6 Restrictions on Access to and Use of the Software

Client will not, and will not permit any third party to:

(a) other than as expressly set forth in the applicable Order, copy, modify, duplicate, create Derivative Works from, frame, mirror, republish, download, transmit, or distribute all or any portion of the Software in any form or media or by any means;

(b) reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software;

(c) access all or any part of the Software in order to build or enhance a product or service which competes with the Software;

(d) other than as expressly set forth in Section 2.2, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Software available to any third party;

(e) take any actions to circumvent standard security practices for accessing and using the Software or to avoid paying amounts due under any Order;

(f) input, upload, transmit, or otherwise provide to or through the Software any information or materials that are unlawful;

(g) access and use any SaaS Product to: (i) interfere with or disrupt the integrity, security or performance of other deployments of the SaaS Product or the data contained therein; or (ii) attempt to gain unauthorized access to other deployments of the SaaS Product or any shared systems, products or networks;

(h) remove, cover-up or obscure any trademark, trade name, copyright notice or other proprietary notice on the Software; or

(i) otherwise access or use the Software beyond the scope of the authorization granted in the Relativity Agreement and the Panoram Agreement.

2.7 Reservation of Rights in the Software

As between the Parties, Conduent and its third-party vendors own and will continue to own the entire title and interest in and to the Software and all Intellectual Property Rights related to the Software, including all Derivative Works thereof, and any know-how, methodologies or other materials Conduent provides. Nothing in the Relativity Agreement or the Panoram Agreement, or the negotiation or performance thereof, grants any right, title or interest in or to the Software or any such Intellectual Property Rights, whether expressly, by implication, estoppel, or otherwise. Client has no right to access any source code.

2.8 Responsibility for Client Systems

Client is solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the data centres, and Conduent and Panoram will not be responsible for resolving any problems, conditions, delays, or delivery failures, or liable for any loss or damage arising from or relating to Client's network connections or telecommunications links or caused by the Internet.

3. BILLING

3.1 Billing Assistance

Client's billing and usage metrics will be delivered to Conduent through the Software as set forth in the Documentation. Client will provide any requested information as may be reasonably necessary for Conduent's billing and auditing purposes, and reasonably cooperate in: (a) running and providing the results of usage and billing scripts; (b) providing Conduent with certifications respecting usage metrics; and (c) granting Conduent remote, supervised, secure access to Client's account to verify billing and usage metrics.

4. DATA

4.1 Client Data

As between Client and Conduent and the Client and Panoram, Client is responsible for the content and use of Client Data, and will remain the sole and exclusive owner of all right, title and interest in and to Client Data, including all Intellectual Property Rights relating thereto.

4.2 Right to Access and Use Client Data

Client grants Conduent a non-exclusive, non-transferable right to access and use Client Data for the purpose of providing the Software and performing Conduent 's obligations under the Relativity Agreement. Client grants Panoram a non-exclusive, non-transferable right to access and use Client Data for the purpose of providing the Software and performing Panoram's obligations under the Panoram Agreement.

4.3 Client Data Security

Conduent shall safeguard Client Data as set forth in the Data Security Terms.

4.4 Usage Data

Conduent may collect, reproduce, distribute, modify, and otherwise use and publish data and other information that Conduent compiles or derives, relating to or arising from the performance or use of the Software by Client and its Authorized Users, including statistics, metrics and analytic data, and any data and other information derived therefrom (collectively, "Usage Data"); provided, however, that, Usage Data shall be anonymized and aggregated, and shall never contain Client Data, any information by which any person would reasonably be able to determine the identity of Client or any other person or party, or any other Client Confidential Information. As between Conduent and Client, Conduent shall be the sole and exclusive owner of all right, title and interest in and to Usage Data, including all Intellectual Property Rights relating thereto.

5. REPRESENTATIONS AND WARRANTIES

5.1 Conduent Representations and Warranties

Conduent represents and warrants to Client that:

(a) it has the right to enter into the Relativity Agreement and grant the rights granted in the Relativity Agreement;

(b) subject to Section 5.2, the Software will perform substantially in conformance with the Documentation (Client's sole and exclusive remedy for any failure by Conduent to meet the representation and warranty set forth in this Section 5.1(b), is to terminate the Relativity Agreement on written notice if it has provided notice to Conduent to remedy the Software where it is not substantially in conformance with the Documentation, and Conduent fails to remedy this to make the Software substantially in conformance with the Documentation within 30 days of that notice;

(c) it will comply with all Laws applicable to its business operations and its provision of the Software to Client;

(d) it will use commercially reasonable software development practices designed to prevent the Software from containing or transmitting any Harmful Code; and

(e) the Software will not contain, and has not been developed or modified through the use of, any open source or public library software, including any version of any software licensed pursuant to any GNU public license, in such a way as to (i) require Client to grant to any third party any rights in Client's products, services or Intellectual Property Rights, (ii) require the licensing, disclosure or distribution of any source code developed by or for Client, (iii) require Client to license the use of its products or services to third parties without charge, or (iv) create restrictions on or immunities to Client's enforcement of its Intellectual Property Rights.

5.2 Disclaimer of Warranties

The representation and warranty set forth in Section 5.1(b) will not apply to: (a) the extent of any non-conformance arising from abuse, misapplication, or other user errors by Client, or any use of the Software not in conformance with the Documentation, or use of the Software in combination or operation with any software, hardware, service, or data not provided by Conduent or Panoram or identified as a specific technical requirement in the Documentation, to the extent the nonconformity would not have occurred in the absence of such combination or operation. Conduent and Panoram do not warrant that the functions or the results of using the Software will be suitable for Client's intended use (including sufficiency, accuracy, reliability or legal compliance), that the operation of the Software will be timely, uninterrupted or error-free, or that the Software will be secure from unauthorized access or hacking or free of Harmful Code. The express warranties made herein are in lieu of, and to the exclusion of, all other warranties, conditions or representations of any kind, express or implied, statutory or otherwise, relating to the Software or Services. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CONDUENT AND PANORAM EXPRESSLY DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY IMPLIED WARRANTIES OR OTHER OBLIGATIONS ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE, AND ALL SUCH WARRANTIES, CONDITIONS AND REPRESENTATIONS ARE EXCLUDED FROM THE RELATIVITY AGREEMENT AND THE PANORAM AGREEMENT AND WAIVED TO THE FULLEST EXTENT NOT PROHIBITED BY LAW.

5.3 Client Representations and Warranties

Client represents and warrants to Conduent and Panoram that:

(a) it has the right to enter into the Relativity Agreement and the Panoram Agreement and grant the rights granted to Conduent and Panoram in the Relativity Agreement and Panoram in the Panoram Agreement;

(b) it will comply with all Laws applicable to its business operations and its provision of Client Data to Conduent and Panoram; and

(c) it will use commercially reasonable practices, including the use of anti-virus and malware protection software, designed to prevent Client Data from containing or transmitting any Harmful Code.

6. TERM AND TERMINATION

6.1 Term

This Relativity Agreement shall continue for the term of the Scope Of Work and upon the termination or expiry of the Scope of Work it shall terminate immediately.

6.2 Effect of Termination or Expiration

Upon any expiration or termination all rights, licenses, consents, and authorizations granted by either party to the other party under the Relativity Agreement (or specific Order/Scope of Work, as applicable) will immediately terminate. Upon any expiration or termination of the Relativity Agreement or any applicable Order, each party will promptly return to other party, or at the other party's request, destroy all documents and tangible materials containing, reflecting, incorporating, or based on Confidential Information of the other party and, except as set forth below, permanently erase all Confidential Information of the other party from all systems it directly or indirectly controls. Client will export or otherwise delete all Client Data in any SaaS Product or Software. If Client fails to export or delete any Client Data in a SaaS Product by the expiration date of the Relativity Agreement or the applicable Order, within ten (10) days of any termination of the Relativity Agreement, Panoram may (a) continue charging Client for access to and use of the SaaS Product at the rates set forth in the applicable Order or (b) delete such Client Data. Notwithstanding anything to the contrary in this section or elsewhere in the Relativity Agreement, a party may retain Confidential Information of the other party, including Client Data, in its then current state and solely to the extent and for so long as required for the receiving party to comply with Laws applicable to its business. In addition, Conduent and Panoram may retain Client Data in their backups, archives and disaster recovery systems until such Client Data is deleted in the ordinary course. Any Confidential Information retained under this Section will remain subject to all confidentiality, security and other applicable requirements of the Relativity Agreement and the Panoram Agreement, as applicable.

7. INDEMNIFICATION

7.1 Indemnification by Client

Conduent will indemnify, defend and hold harmless Client, its Affiliates and its and their Representatives ("Client Indemnified Parties") from and against any Losses incurred in connection with any third-party Claim against the Client Indemnified Parties to the extent that such Losses arise out of or result from any allegation that, if true, would constitute infringement, misappropriation or other violation of any third-party Intellectual Property rights resulting from use of the Software pursuant to the terms of the Relativity Agreement (an "IP Claim").

7.2 Indemnification by Client

Client will indemnify, defend and hold harmless Conduent and Panoram, their Affiliates and their Representatives ("Conduent and Panoram Indemnified Parties") from and against any Losses incurred in connection with any third-party Claim against Conduent and Panoram Indemnified Parties to the extent that such Losses arise out of or result from:

(a) any allegation with respect to Client Data that, if true, would constitute, or would result from, violation by Client or its Authorized Users of any applicable data privacy or data protection Laws or any obligation of confidentiality to any third party;

(b) any allegation that if true, would constitute infringement, misappropriation or other violation of any third-party Intellectual Property Rights.

7.3 IP Claims Limitations and Mitigation

Conduent and Panoram will have no liability or obligation for any IP Claim or Losses to the extent that such IP Claim arises out of or results from any: (a) access to or use of the Software other than as authorized under the Relativity Agreement and the Panoram Agreement; (b) alteration or modification of the Software by Client or any Authorized User; or (c) use of the Software in combination or operation with any other software, hardware, service, or data not provided by Conduent or Panoram or identified as a technical requirement in the Documentation, to the extent the IP Claim could have been avoided in the absence of such combination or operation.

If the Software is, or Conduent believes the Software is likely to be, the subject of an IP Claim, Conduent may, at its option and expense: (i) obtain for Client a license to continue using the Software; (ii) modify the Software, without materially affecting the functionality; (iii) obtain for Client a license to use other software which is marketed to compete with the Software; or (iv) terminate the applicable Order and refund a pro-rated portion of any fees prepaid by Client for access to and use of the relevant Software or any related Services, with the pro-rated period commencing on the date Client discontinued use of the Software due to the IP Claim.

This Section 7 contains the only liability and obligations of Conduent, and the only remedies of Client, for IP Claims.

7.4 Indemnification Procedure

If a party receives notice of a Claim for which it is indemnified, it will forward the notice to the other party within 15 days (provided that any failure to notify will relieve the indemnifying party of its indemnification obligations only to the extent that such failure actually prejudices its defense of the Claim). The indemnifying party will: (a) promptly assume sole control of the defense of the Claim and will employ counsel of its choice to handle and defend the Claim; and (b) not settle any Claim without the prior written consent of the indemnified party (which will not be unreasonably withheld, delayed or conditioned), unless such settlement is solely for money damages, includes an unconditional release of the indemnified party from all liability for claims that are the subject matter of the Claim, and does not impose any obligations upon, or prejudice the rights of, the indemnified party. The indemnified party will: (i) provide cooperation and assistance to the indemnifying party, at the indemnifying party's expense; and (ii) not settle or compromise the Claim or make any admission or substantive response relating to the Claim that materially prejudices the indemnifying party's ability to defend the Claim, so long as the indemnifying party is defending or seeking to settle or compromise the Claim through qualified counsel. Subject to the foregoing, except in the case of an IP Claim, the indemnified party may participate in and observe the proceedings, at its own expense, with counsel of its own choosing.

8. LIMITATION OF LIABILITY

8.1 EXCLUSION OF DAMAGES

TO THE EXTENT PERMITTED BY LAW, AND EXCEPT AS SET FORTH IN SECTION 8.4, IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER OR IN CONNECTION WITH THE RELATIVITY AGREEMENT FOR ANY: (A) LOSS OF USE, BUSINESS, REVENUE OR PROFIT OR DIMINUTION IN VALUE; (B) IMPAIRMENT OF, INABILITY TO USE OR LOSS, INTERRUPTION OR DELAY OF THE SOFTWARE (OTHER THAN AS SET FORTH IN ANY SERVICE LEVEL TERMS), OR LOSS OR BREACH OF INFORMATION OR DATA; (C) COST OF REPLACEMENT GOODS OR SERVICES; (D) LOSS OF GOODWILL OR REPUTATION; OR (E) EXCEPT

AS OTHERWISE SET FORTH HEREIN, CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED OR PUNITIVE DAMAGES.

8.2 GENERAL CAP ON LIABILITY

EXCEPT AS SET FORTH IN SECTION 8.3, IN NO EVENT WILL THE AGGREGATE LIABILITY OF A PARTY UNDER AN ORDER EXCEED THE TOTAL AMOUNT PAID OR PAYABLE TO CONDUENT UNDER THE APPLICABLE ORDER FOR THE 12 MONTH PERIOD THAT PRECEEDED THE EVENT THAT GAVE RISE TO THE FIRST CLAIM FOR DAMAGES UNDER THAT ORDER ("GENERAL CAP").

8.3 EXCLUSIONS

SECTION 8.2 WILL NOT APPLY TO LIABILITY ARISING OUT OF OR RELATING TO A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS AS TO CONFIDENTIAL INFORMATION AS SET FORTH IN THE RELATIVITY AGREEMENT, CLIENT'S BREACH OF SECTION 2.6 (RESTRICTIONS ON ACCESS TO AND USE OF THE SOFTWARE), CLIENT'S OBLIGATION TO PAY FOR SOFTWARE OR SERVICES UNDER THE RELATIVITY AGREEMENT, A PARTY'S OBLIGATIONS UNDER SECTION 7 (INDEMNIFICATION) OF THESE MASTER TERMS, A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR A PARTY'S VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS. FOR THE AVOIDANCE OF DOUBT, A PARTY'S BREACH OF THE DATA SECURITY TERMS RESULTING IN A DATA BREACH (AS DEFINED IN THE DATA SECURITY TERMS) SHALL NOT BE TREATED AS A BREACH OF CONFIDENTIALITY (I.E., A DATA BREACH CLAIM IS NOT AN UNCAPPED CLAIM UNDER THIS SECTION).

8.4 APPLICABILITY OF LIMITATIONS OF LIABILITY

THE LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION 8 WILL APPLY, TO THE EXTENT PERMITTED BY LAW, (A) WHETHER THE APPLICABLE CLAIM ARISES UNDER BREACH OF CONTRACT, TORT, STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY, (B) WHETHER THE CLAIMANT WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES, OR SUCH LOSSES WERE OTHERWISE FORESEEABLE, AND (C) EVEN IF EVERY OTHER REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9. PUBLICITY

Neither party will issue or release any announcement, statement, press release, or other publicity or marketing materials relating to the Relativity Agreement or the Panoram Agreement or, unless expressly permitted under the Relativity Agreement or the Panoram Agreement, otherwise use the other party's trademarks, service marks, trade names, logos, domain names, or other indicia of association, in each case, without the prior written consent of the other party. Any permitted use of a party's name and logo shall be in compliance with any written guidelines provided by the party regarding use of its name and logo, and each party agrees to remove the name and logo promptly after the other party's written request which provides a reasonable basis for objecting to continued use.

10. FEEDBACK

Subject to the obligations set forth in the Relativity Agreement, Conduent may use any suggestions, ideas, enhancement requests, recommendations or other feedback relating to Conduent or to the Software (collectively, "Client Feedback") for purposes of modifying the Software, creating Derivative Works, or creating new products or services (collectively, the "Improvements"). Conduent will own exclusively all Improvements including those based upon or incorporating Client Feedback, without any obligation to pay Client any royalty or other compensation. Conduent's use of Client Feedback will be at Conduent's sole risk without any representations, warranties or liability of Client and shall not use or incorporate any Confidential Information of Client or Client Data, including but not limited to the customers or clients of Client.

11. GOVERNING LAW, JURISDICTION AND RELATED MATTERS

11.1 Governing Law and Jurisdiction. The Relativity Master Terms will be governed by and interpreted in accordance with the Laws of the State of New York USA, without regard to any choice of law or conflicts of laws provisions. All claims and disputes under the Relativity Master Terms will be litigated, at the election of the party initiating litigation, exclusively in the state of New York. The parties irrevocably submit to the jurisdiction and venue of the federal and state courts located in such jurisdiction and agree that such courts are convenient forums. Under no circumstances will the "Uniform Computer Information Transactions Act," the American Law Institute's "Principles of the Law of Software Contracts," as model laws or as adopted in any jurisdiction, or the United Nations Convention on Contracts for the International Sale of Goods, or similar acts, laws and conventions have any bearing on the interpretation or enforcement of the Relativity Master Terms and the parties hereby elect to opt out of all such acts, laws and conventions.

11.2 Waiver of Jury Trial

Each party irrevocably and unconditionally waives any right it may have to a trial by jury in any court action, proceeding or counterclaim by either party against the other party arising out of or relating to the Agreement.

11.3 Export Restrictions

The Software is subject to U.S. export control laws (regardless of Client's domicile or location) and may be subject to export or import requirements in other countries. Without limiting any other Section of the Relativity Agreement relating to compliance with applicable Laws, Client will comply with, and take all action necessary to effect its compliance with, all applicable export, re-export, and import laws, including the U.S. Export Administration Regulations. Client will not permit access to the Software or transfer, export or re-export of the Software, or the underlying information or technology, by or to any person or other party in violation of US legal restrictions, including any party who is a national or resident of, or located in, any country on the United States Department of Treasury's List of Specially Designated Nationals and Blocked Parties or the U.S. Department of Commerce's Table of Denial Orders, or similar lists identifying parties sanctioned by the U.S. government or any locally applicable denied party lists.

11.4 Assignment

Neither party may assign its rights or obligations under the Relativity Agreement without the prior written consent of the other party, which will not be unreasonably withheld, conditioned or delayed. Any Change in Control will be considered an assignment for purposes of this provision. "Change in Control" means any change in the persons or entities controlling a party, including such changes resulting from a merger, consolidation or stock transfer. Notwithstanding the foregoing, either party may assign the Relativity Agreement to an Affiliate or to any third party into which the assigning party is merged, consolidated or reorganized, or to which all or substantially all of the assigning party's assets are sold, upon written notice to the other party, so long as the transferee expressly assumes all obligations of the assigning party under the Relativity Agreement; provided, however, that, Client may not assign this Relativity Agreement to any Competitor without Conduent and Panoram's prior written consent.

"Competitor" means any person or entity that provides software or services for use in connection with eDiscovery, document review, case management, internal investigations or communications surveillance, but excluding any entity whose primary business is providing legal advice. A Competitor includes any Affiliate of a Competitor. If, upon receipt of a request to assign this Relativity Agreement, Conduent reasonably determines that the proposed assignee is a Competitor, Conduent will notify Client of its objection to the proposed assignee and any such assignment shall be null and void. The Relativity Agreement will be binding upon and inure to the benefit of the parties' successors and permitted assigns.

12. ADDITIONAL TERMS

Documents incorporated by reference	
Data Security Terms	Attached as Exhibit A

EXHIBIT A - to Schedule 3

DATA SECURITY TERMS

I. DEFINITIONS

Capitalized terms used in these Data Security Terms but not defined have the meanings set forth in the Master Terms and Conditions or the applicable Order.

II. CLOUD VENDOR DATA SECURITY CONTROLS

Conduent's licensor (Relativity) (Relativity and Conduent, both singly and collectively, as used herein, "Licensor") uses a cloud vendor to provide the infrastructure environment to run the SaaS Product (the "Cloud Vendor"). The current Cloud Vendor is Microsoft Azure. Accordingly, the SaaS Product currently operates within Microsoft Azure's security framework. Details on Microsoft Azure's security, privacy, and compliance standards may be found on the Microsoft Azure Trust Center homepage: https://azure.microsoft.com/en-us/support/trust-center/. Licensor reserves the right to switch to a different Cloud Vendor or to a data center that Licensor or its affiliate operates, provided the data security arrangements shall be at least consistent with prevailing industry standards and the provisions in these Data Security Terms and the security of Client Data shall not be materially diminished. Licensor will provide at least 90 days' advance notice to Client of any change in Cloud Vendor. Current Cloud Vendor security certifications include ISO 27001, SOC 2 and HIPAA Privacy and Security Rules (via HITRUST CSF). As part of the process for obtaining and maintaining these certifications, the Cloud Vendor has implemented numerous procedures, including: (a) personnel background checks and security awareness training; (b) physical and logical access control safeguards; (c) incident response plans; and (d) disaster recovery and business continuity plans.

III. AUTHORIZED USER ACCESS AND PERMISSIONS

Within the SaaS Product, Client's Admins can choose from numerous local and external identification authentication methods and resource options to help secure the process of granting, controlling and revoking user access. Admins can also view case access and permission audits to ensure that Authorized Users have the proper level of permissions. The SaaS Product's object security model means that Admins can manage varying levels of security for objects such as views, tabs and fields, across Client's Geo and in each workspace. The SaaS Product's group permission model allows Admins to quickly apply or modify security profiles for a number of Authorized Users simultaneously by assigning permissions at group level. After configuring a group's access permissions, Admins can preview the effective security rights by impersonating a general member of the group or a specific user. More details on such permission controls are included in the Documentation.

IV. RELATIVITY DATA SECURITY PROCEDURES

1. OVERVIEW

While no business can prevent all potential hacking or other criminal conduct, and the Cloud Vendor has certified infrastructure safeguards, Licensor also maintains its own security program with administrative, technical, and physical safeguards. Licensor's security program, together with the Cloud Vendor's security program, is designed to:

- protect the confidentiality, integrity and availability of Client Data in Licensor's possession or control or to which Licensor has access in the SaaS Product;
- protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Client Data;
- protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Client Data;
- protect against accidental loss or destruction of, or damage to, Client Data; and
- safeguard Client Data as required by any Laws which apply to Licensor based on Licensor's operations in processing Client Data.

Without limiting the generality of the foregoing, Licensor's security program, which is in addition to the Cloud Vendor's security program, currently includes the elements described in Sections 2 through 17 below.

2. SECURITY CERTIFICATIONS AND AUDITS

Licensor will maintain a certificate from a reputable third-party certification authority of Licensor's compliance with ISO / IEC 27001: 2013 or any successor standard. Licensor will also obtain and maintain an SSAE18 SOC 2, Type II audit report covering any system or process that stores or processes Client Data and any system that could pose a risk to such systems and processes. Promptly after receiving written requests from Client up to once per year, Licensor will provide a copy of its most recent third-party ISO certification or audit summary, or SSAE18 SOC 2, Type II audit report, or any recent third-party penetration test attestations or summary statements. Further, upon request, Licensor will provide Client with the most current version of its Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CSA CAIQ) relating to Licensor's then-current operation of the SaaS Product.

3. SECURITY TRAINING, CONFIDENTIALITY OBLIGATIONS AND BACKGROUND CHECKS

Licensor provides a mandatory security and privacy awareness and training program for all Licensor employees and any persons working as contractors who may have access to Client Data in the performance of their services (collectively, "Workers With Access"). All Workers With Access are also subject to confidentiality obligations. Further, Licensor conducts background checks consistent with prevailing practices for similar companies in connection with the hiring or engaging of all Workers With Access. Licensor will not hire or engage any Worker With Access if the background check shows that the individual was convicted of a crime involving theft, dishonesty, fraud or computer-related crimes. Licensor's commitments with respect to background checks are subject to all applicable Laws pertaining to such background checks.

4. ENCRYPTION PROGRAMS

4.1 Encryption Policy

Licensor has a documented security cryptography policy that dictates encryption use, applicable encryption standards, and encryption strength.

4.2 Encryption in Transit

Encryption in transit utilizing standard encryption technology (e.g., Transport Layer Security (TLS), IPSec, and SMB).

4.3 Email Encryption

The SaaS Product has a default setting so that email messages between Client and Licensor are encrypted leveraging Transport Layer Security (TLS). Encryption technology used adheres to applicable legal requirements governing the use of such technology. Email messages to Client's Authorized Users who do not use Client's email domain are encrypted by Opportunistic TLS.

4.4 Encryption at Rest

All Client Data at rest is encrypted using industry standard symmetric encryption.

5. ANTI-MALWARE SERVICES

Licensor leverages third-party anti-malware program services to help protect against malware impacting system services and functions, as further described below.

- Licensor provides, supports and maintains an anti-malware service.
- Licensor's anti-malware service is configured to automatically scan files that are accessed by the SaaS Product servers and storage services by untrusted processes (the process itself is scanned).
- Licensor's anti-malware service is configured to log all scanning activity. Upon the detection of a suspected malware infected file, Licensor's anti-malware service is configured to automatically quarantine the infected file and generate an associated log entry.
- Upon the detection and quarantine of a suspected malware infected file, Licensor's anti-malware service is configured to issue an alert to Licensor's monitoring team.

6. PHYSICAL SECURITY

Licensor maintains locked perimeter doors and requires that personnel use electronic key cards and other

reasonable measures designed to ensure that physical access to the Licensor premises is limited to properly authorized individuals. The Cloud Vendor maintains physical access security controls for the data center, including layers of defense-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communications networks.

7. DATA DISPOSAL

Client may delete or export Client Data from the SaaS Product from time to time in Client's discretion and will do so in any event at the end of the Subscription Term for the applicable Order. Upon receiving Client's written request to decommission a Geo, Licensor will follow the secure deletion or disposal procedures in its applicable standard operating procedures respecting any remaining Client Data contained in the decommissioned Geo, the associated disaster recovery Geo in the back-up data center and any related media. Deletion or disposal means the Client Data is rendered inaccessible, undecipherable or otherwise unrecoverable, provided that Licensor may retain copies of Client Data in accordance with Section 10 (Disaster Recovery and Business Continuity Plans), or as otherwise necessary to perform its obligations under the Agreement, including the short term recovery of Client Data at Client's request. Licensor may retain platform monitoring, usage and performance metrics, and security logs, none of which include Client Data.

8. OTHER ACCESS CONTROLS

As further described under Section 9 (Access Control and Password Management Policy), Licensor has policies, procedures, and logical controls designed to limit access to the SaaS Product to properly authorized personnel on a "need to know" basis, to prevent those personnel who should not have access from obtaining access and to remove access of personnel on a timely basis in the event of a change in job responsibilities or job status. For Workers With Access, Licensor's standard operating procedures further limit such access to resolving issues with system components rather than viewing any Client Data (except in situations when incidental viewing of Client Data may be required in connection with resolving an issue or responding to a Client request). Licensor logs such access for at least one (1) year (the first 90 days of which is in readily available hot status, and the remainder of which is in cold storage), and will make such logs available to Client for review to the extent those logs reveal access to Client Data.

9. ACCESS CONTROL AND PASSWORD MANAGEMENT POLICY

9.1 General Password Requirements

Licensor has an Access Control and Password Management Policy and an automated password management system to enforce the policy requirements. The policy covers all applicable systems, applications, and databases. There are classes of password use in Licensor's enterprise and SaaS Product environments, as further detailed below. Industry standard prevailing password practices are deployed to protect against unauthorized use of passwords, including: (a) minimum password length; (b) password complexity; (c) password history; (d) password lockout for failed password attempts; and (e) randomly generated initial passwords.

9.2 Licensor Enterprise Identity and Password Management

The Licensor enterprise uses a single sign-on multi-factor authentication service (currently Okta) for authenticating all individuals in the organization and for authenticating access to the systems that support and operate the SaaS Product (the "Back-End").

(a) **Front-End Access**. Licensor employs the following methods respecting access to the user interface (the "Front-End"):

- Client controls Front-End logins to its Geo through a password management system that employs the user authentication provider, e.g., Active Directory. Client controls Front-End password policies for Client's Authorized Users and can choose from any supported authentication provider in the SaaS Product, including length, expiration, reuse, and complexity requirements, lockout, and reset options.
- Licensor supports integration with OIDC and some SAML Single Sign-On providers to restrict access through the Front-End.
- Licensor personnel who need Front-End access as systems administrators are subject to a gating arrangement consisting of technical and organizational controls designed to prevent such

personnel from accessing Client Data without Client's consent.

(b) **Back-End Access.** Licensor employs the following methods respecting access to the Back-End:

- All TCP connections to Back-End resources are brokered through a privileged access management solution, which logs the unique user ID that created the connections. Only members of specific Licensor Active Directory groups can access Back-End accounts through the privileged access management solution, and all access to this solution requires authentication through a single sign-on multi-factor authentication service (currently Okta). When Licensor personnel access the Back-End, they use shared system and application accounts to authenticate to the SaaS Product servers. Licensor has technical and administrative controls in place to manage risks from the use of such shared system and application accounts and to track such usage. With this privileged access management system, Authorized Users cannot see the credentials; they only launch the TCP connections.
- Licensor service accounts are used by the system to run Back-End processes for the SaaS Product and may require occasional access by Licensor personnel for support and maintenance on a limited need-to-know basis, e.g., to restart a stuck processing worker agent process. Any such access requires a properly credentialed login. Licensor has technical and administrative controls in place to manage risks from the use of shared IDs and to track such usage.

10. DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

The Cloud Vendor and Licensor have disaster recovery and business continuity plans in place, and Licensor has established RTO and RPO timelines as set forth in the Service Level Terms. These plans include a separate back-up data center (which may be in a separate country) and a formal framework by which an unplanned event will be managed to minimize the loss of vital resources. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (a) perform back-up of Client Data to a separate back-up data center in a scheduled and timely manner; (b) provide effective controls to safeguard backed-up Client Data; (c) securely transfer Client Data to and from the back-up location; and (d) fully restore applications and operating systems; (e) demonstrate periodic testing of restoration from the back-up location. If Licensor makes back-ups to tape or other removable media, all such back-ups shall be encrypted in compliance with the encryption requirements set forth above.

11. ASSIGNED SECURITY RESPONSIBILITY

Licensor assigns responsibility for the development, implementation, and maintenance of its security program, including:

- designating a security official with overall responsibility;
- defining security roles for individuals with security responsibilities;
- performing risk assessments of Licensor and the SaaS Product at least annually and whenever major changes to systems or processes occur; and
- designating a Security Governance Committee consisting of cross-functional management representatives to meet on a regular basis.

12. SECURE CODING PRACTICES

All Licensor developer personnel are required to take a course in security awareness and secure coding, and Licensor's coding standards have a strong security component. Among other things, the OWASP Secure Coding Practices Reference are integrated into Licensor's coding standards. The coding standards are reviewed annually and maintained by the architecture and security teams to remain up to date and enforce the prevailing standards. Standard production source code changes go through a pull request workflow to ensure peer review for code quality and adherence to coding standards. Each commit into a Licensor code base requires an approval from another engineer. The approver reviews for compliance with Licensor's coding standards prior to accepting any code change. For new features, completion of a structured review process with Licensor's security team is required. During this process, each project receives a risk rating based on risk ranking criteria. The higher the risk rating, the more security scrutiny the project is subject to during its lifecycle.

13. SECURITY TESTING

Licensor regularly tests the key controls, systems and procedures of its security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Testing currently includes:

- Internal risk assessments
- Network configuration tests
- Use of internal security specialists and/or a third party to conduct web application level security assessments. These assessments generally test for the OWASP Top 10, which may include the following:
    - Cross-site request forgery
    - Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing)
    - XML and SOAP attacks
    - Weak session management
    - Data validation flaws and data model constraint inconsistencies
    - Insufficient authentication
    - Insufficient authorization
    - Web application penetration testing:
        - During web application penetration testing, a dedicated penetration testing team looks for security suspects, such as XSS, Cross Site Request Forgery, authentication issues, and authorization issues. Licensor uses industry standard tests alongside specialized tests, sometimes customized for new features. The penetration testing team also leverages other penetration testing techniques based on their disparate experiences and knowledge of the SaaS Product.
        - On an annual basis, Licensor engages an external penetration testing firm for an extensive test covering the functionality of the SaaS Product, including industry standard tests like those from the OWASP, and additional tests that the penetration testing firm deems necessary as it explores the application.
        - Upon request, Licensor will provide Client with an annual penetration test attestation letter.

14. SECURITY MONITORING & AUTOMATED VULNERABILITY SCANS

Licensor monitors network and production systems, including error logs on servers, disks and security events for any suspicious or malicious activities. Monitoring generally includes:

- Arranging for automated vulnerability scans of any assets deployed in the SaaS Product that contain Client Data, to be performed periodically to identify, mitigate or remediate any vulnerabilities. Assets include any servers, applications, and if applicable, endpoint desktops, laptops and network devices.
- Subscribing to vulnerability intelligence services or to information security advisories and other relevant sources providing current information about system vulnerabilities (none of which involves the submission of any Client Data).
- Reviewing changes affecting systems handling authentication, authorization, and auditing.
- Reviewing privileged Back-End access to the SaaS Product to validate privileged access is appropriate.
- Engaging third parties to perform network vulnerability assessments and penetration testing on an annual basis.
- Maintaining industry standard event logging for servers, applications, and networking equipment to facilitate security incident and event management. Licensor maintains such logs for at least one (1) year (the first 90 days of which is in readily available hot status, and the remainder of which is in cold storage).
- Classifying vulnerabilities in accordance with industry standard risk rating methodologies (e.g., the Common Vulnerability Scoring System, OWASP, or NIST).

- Mitigating and/or remediating vulnerabilities in the SaaS Product infrastructure or applications that could allow direct unauthorized access to Client Data, whether by applying an available patch or taking other reasonable actions, in the following time frames:

Severity	Policy	
	Licensor SaaS Product	**Third-Party Software**
Critical	Before the software is released if found in release testing. Within 7 days of identification of vulnerability if found after release.	Within 7 days of receiving notice of patch availability from the third-party vendor and up to 15 days for testing.
High	Before the software is released if found in release testing. Within 30 days of identification of vulnerability if found after release.	Within 30 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing.
Medium	Within 90 days of identification of vulnerability.	Within 90 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing.
Low	Within 180 days of identification of vulnerability.	Within 180 days of receiving notice of patch availability from the third-party vendor and up to 60 days for testing.

Upon request, Licensor will provide Client with an annual vulnerability test summary report.

15. CHANGE AND CONFIGURATION MANAGEMENT

Licensor maintains policies and procedures for managing changes to the SaaS Product. Policies and procedures include:

- a process for documenting, testing and approving the promotion of changes into production; and
- a security patching process that requires patching systems in a timely manner based on a risk analysis.

16. SECURITY INCIDENT RESPONSES

16.1 Cyber Team

Licensor has a Cyber Team that: (a) is capable of meeting on short notice to address any incidents; and (b) focuses on continuous development and improvement of procedures to be followed in the event of any security breach of Client Data or any security breach of any application or system directly associated with the accessing, processing, storage, communication or transmission of Client Data. Procedures currently include:

- Roles and responsibilities: Licensor's Cyber Team will act in coordination with additional security and engineering resources throughout the incident response process;
- Investigation: assessing the risk the incident poses and determining who may be affected;
- Communication: internal reporting as well as the Data Breach notification process set forth below;
- Recordkeeping: keeping a permanent record of what was done and by whom to help in later analysis and possible legal action; and
- Audit: conducting and documenting root cause analysis and remediation plans.

16.2 Security Incident Response

(a) **Notification of a Data Breach.** Unless notification is delayed or prohibited by the actions or demands of a law enforcement agency, Licensor will report a Data Breach to Client's security contact designated to Licensor within 24 hours following determination by Licensor that such an incident has occurred, or that Licensor reasonably suspects may have occurred. "Data Breach" means: (i) the unauthorized acquisition, access, use, disclosure, or destruction or impairment of Client Data that Licensor determines has occurred; or (ii) the unauthorized acquisition, use, disclosure, or destruction or impairment of Client Data that Licensor reasonably suspects may have occurred but which it cannot definitively conclude occurred.

(b) **Licensor Response.** Licensor will take reasonable measures to promptly mitigate the cause of any Data Breach, implement any appropriate monitoring protocol and identify the circumstances that allowed the Data Breach to happen in order to help prevent any further similar Data Breaches (unless the Data Breach was caused by the acts or omissions of Client or any of its Authorized Users, in which case Client shall take such actions). Licensor may work with forensic investigators, law firms and law enforcement agencies to help determine the nature, extent and source of any Data Breach and may make any disclosures of security records, security logs and other information that Licensor deems appropriate or is required to make under applicable Laws (provided any disclosures of Client Data shall require Client's prior written consent, except to the extent that Licensor would risk fines or other sanctions or liabilities for withholding the information). If Licensor makes any statements about a Data Breach without the approval of Client, Licensor will not disclose that Client or Client Data was involved, unless such disclosure is required by applicable Law.

(c) **Cooperation with Client.** Upon Client's request, Licensor will cooperate with Client (and Client's regulators and insurers) to investigate the Data Breach and seek to identify the specific Client Data involved in the Data Breach (without charge, except to the extent the Data Breach was caused or contributed to by the acts or omissions of Client or its Authorized Users). Unless prohibited by applicable Law, Licensor will: (i) provide information regarding the nature and consequences of the Data Breach as such information is collected or otherwise becomes available to Licensor; and (ii) otherwise reasonably assist Client to notify affected individuals, government agencies, regulators and/or credit bureaus; provided, the parties agree that Client is solely responsible for determining whether to notify impacted owners of the Client Data and if regulatory bodies or enforcement commissions applicable to Client or Client Data need to be notified, and for providing such notices.

(d) **Access Credentials.** For clarity, Client is responsible for safeguarding its Access Credentials under the Master Terms and Conditions; any breach of such obligation shall constitute a breach of these Data Security Terms by Client.

17. ADJUSTMENT TO THESE DATA SECURITY TERMS

Licensor monitors and evaluates its security program on a regular basis and may adjust it and these Data Security Terms from time to time, as appropriate in light of: (a) prevailing practices; (b) any relevant changes in technology and any internal or external threats to Licensor or the Client Data; and (c) Licensor's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.