Gen™ is a global company with a family of consumer brands including Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner.

Procurement Terms and Conditions

OFFER AND ACCEPTANCE. These Procurement Terms and Conditions including all exhibits and attachments, and all terms stated explicitly or incorporated by reference herein and/or therein ("**Terms**") constitute an offer by Gen Digital Inc. and its affiliates ("**Gen**") to purchase on a non-exclusive basis the goods, services, licenses, entitlements, Deliverables and results of services described in the corresponding purchase order (individually and collectively referred to as the "**Solutions**") solely as provided under these Terms. The seller or provider of such Solutions together with its affiliates ("**Supplier**") conclusively accepts this offer and these Terms by either performing or delivering the Solutions or promising to perform or deliver the Solutions.

SUPPLIER'S ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS. GEN OBJECTS TO AND HEREBY FULLY REJECTS ANY AND ALL GOVERNING TERMS PROPOSED BY SUPPLIER (OR ATTEMPTED TO BE IMPOSED BY SUPPLIER), INCLUDING WITHOUT LIMIT IN ANY QUOTE, INVOICE, ORDER, CONFIRMATION, OR IN ANY 'CLICK-TO-ACCEPT' OR SHRINK-WRAP LICENSES OR TERMS, WHETHER IN HARD COPY OR ELECTRONIC FORM. SUPPLIER AGREES THAT ANY SUCH ADDITIONAL OR DIFFERENT TERMS, WHETHER RECEIVED PRIOR TO OR AFTER THE DATE OF THESE TERMS, ARE HEREBY REJECTED BY GEN AND BY SUPPLIER AND WILL BE DISREGARDED AND DEEMED TO BE FULLY NULL AND VOID AND UNENFORCEABLE UNLESS SUCH TERMS ARE EXPLICITY AGREED TO IN A SEPARATE MUTUALLY SIGNED AGREEMENT EXECUTED BETWEEN THE PARTIES TO GOVERN THE CORRESPONDING PURCHASE/PURCHASE ORDER.

1. Performance. Notwithstanding anything to the contrary, these Terms exclusively govern Supplier's provision of Solutions to Gen, which will be provided as set forth in each mutually executed order form or statement of work between the parties, or corresponding purchase order if no such order form or statement of work exists ("**Order**"). Supplier is responsible and liable for the acts, omissions, and breaches by its employees, contractors, suppliers and other third parties engaged by or for Supplier (individually and collectively, "**Personnel**"). In addition, Supplier (and not Gen) is responsible for all fees, reimursement, compensation, benefits, taxes and other amounts due to its Personnel or to a third party (including without limit government bodies) on account of its Personnel.

2. Payment. Undisputed fees are due within sixty (60) days of receipt of invoice. Invoices must include the respective purchase order number and line-item descriptions and must be submitted to Gen no later than sixty days (60) following the date when such amounts and expenses are incurred. Orders and Solutions may only be renewed or extended if and as agreed in a subsequent renewal Order together with Gen's issuance of corresponding purchase order, and not by automatic renewal. Expenses will be reimbursed only if and up to the amount specified in an Order, and only in compliance with **Gen's Travel and Expense Policy** at www.nortonlifelock.com/us/en/procurement/supplier-travel-and-expense-policy/ which terms are fully incorporated herein. Notwithstanding anything to the contrary, Supplier may not provide Solutions, or incur or invoice any amounts, unless and until an Order has been fully executed for the Solutions and Gen has delivered a corresponding purchase order for such amounts. Supplier may not invoice or collect any amounts not incurred or invoiced in compliance with this Section. Gen will pay all taxes assessed against or due in connection with these Terms (excluding those due on Supplier's income). If Gen pays withholding taxes in connection with these Terms, it may deduct such amount from amounts otherwise due hereunder (with the net payment constituting payment in full) and, on Supplier's request, will provide payment documentation sufficient for Supplier to request a credit for such amount.

3. Confidentiality. "Confidential Information" means all (a) Personal Data (defined below) and (b) non-public information, data, content and materials (in any form or format) about a party and/or their business, including without limit their Personnel, customers and other third parties, products, services, software, processes or security, or their marketing, financial and other business plans or information, and any other information, data, content and materials identified at the time of disclosure as confidential or proprietary, or which otherwise one would reasonably expect to be confidential or proprietary. To avoid doubt, Gen's requirements and all Deliverables are Gen's Confidential Information. Confidential Information may only be used by a recipient in performance under these Terms and the applicable Order, and with at least a reasonable degree of care. As between the parties, all right, title and interest in and to Confidential Information will remain solely with the discloser. Neither party may allow a third party to access or use the other party's Confidential Information except for their respective Personnel who have a need to know and are under binding obligations of non-disclosure that are substantially as protective of such Confidential Information as are these Terms. Supplier will notify Gen immediately and in reasonable detail if it believes that Gen's Confidential Information has been subject to unauthorized use or access and will take corrective action as appropriate, and as reasonably requested by Gen. On termination of an Order or at a party's earlier request, the recipient shall promptly return (and destroy, if requested) the discloser's Confidential Information at no cost. Confidential Information does not include information that the recipient can demonstrate became publicly available through no fault, act or omission by the recipient, or that was independently developed by the recipient or rightfully received from a third party with no obligation of nondisclosure. In addition, a recipient may disclose Confidential Information to the extent required by law, provided that it must promptly notify the discloser (unless legally prohibited) and cooperate with the discloser's request to limit or re-direct the request, at discloser's cost. If Gen is legally compelled to produce Gen Confidential

Information that is hosted by, or otherwise within Supplier's possession or control, Supplier will promptly and reasonably cooperate to produce such information in a timely manner. Where the burden on Supplier for such cooperation is no longer reasonable the parties will negotiate an appropriate allocation of cost in good faith, and not as a contingency to cooperation.

4. Personal Data. If Supplier processes Personal Data for or on behalf of Gen as part of its provision of Solutions, the terms of the **Gen Data Processing Agreement ("DPA")** attached as **Exhibit A** apply in addition to these Terms and are fully incorporated herein. If Supplier uses or provides tracking technologies (including without limit pixels, tags or web beacons) in the provision of Solutions, Supplier must: (i) notify Gen about the type of tracking technology used and the information collected, (ii) collect information and use information gained exclusively to provide the Solutions; and (iii) enable (or allow Gen to enable) appropriate mechanisms for data subjects to opt-in and opt-out of such tracking technologies, and provide accurate and complete disclosures prior to the collection of information in accordance with applicable laws. "**Personal Data**" has the meaning assigned in the DPA.

5. Data Security. Supplier will maintain, at a minimum, the technical and organizational measures and controls specified in **Gen's Master Supplier Security Requirements ("MPSR")** attached as **Exhibit B** which terms are fully incorporated herein, and Supplier will update those with equivalent or more protective measures and controls as needed to remain compliant at all times with then-current industry standard practices.

6. Designated Solutions. If Supplier Personnel provide Solutions on Gen designated premises or access Gen's Confidential Information or networks (individually and collectively '**Designated Solutions**"), the following terms apply:

a. Supplier Personnel will comply with Gen's work rules and policies as provided by Gen, and shall not copy or remove Gen materials, data or property from Gen's premises or networks without first obtaining Gen's express consent.
b. On Gen's request, Supplier will promptly replace individual Personnel who are working on Gen designated premises with appropriately skilled and qualified individuals. Gen will not be invoiced or obligated to pay an increased rate for the replacement Personnel or for any time or expenses incurred to train and familiarize such replacement with the applicable engagement.
c. Before Supplier Personnel perform Designated Solutions, Supplier warrants that: (i) to the extent permitted by local law, it will perform (and will obtain appropriate consent to perform) appropriate background investigations, including without limit as may be set forth in Gen's Master Supplier Security Requirements, (ii) no information was discovered in such investigation(s) that could be reasonably construed to negatively impact performance or result in breach of these Terms, and (iii) Supplier will confirm (in writing) its compliance with this section on Gen's request. Gen reserves the right to refuse access to its premises and network(s) at any time, for any lawful reason.

7. No Publicity; Trademarks. Supplier shall not make any direct or implied reference to Gen or use Gen's names, logos or trademarks for any sales, marketing, or publicity purposes. If Gen requires that Supplier use any Gen trademarks as part of its provision of Solutions, Supplier will fully comply with Gen's branding and trademark use guidelines https://www.nortonlifelock.com/us/en/legal/trademark-policies/ which terms are fully incorporated herein, and as otherwise explicitly specified in an applicable Order. Gen reserves to itself all other rights not specified therein.

8. Acceptance. If Solutions or any portion thereof are subject to acceptance review by Gen as indicated in the applicable Order or otherwise explicitly agreed by the parties in writing, the following terms apply:

a. Unless otherwise agreed in the applicable Order, Supplier will notify Gen when Solutions are ready for Gen's review. Gen will within 15 days of its receipt, inform Supplier of whether it accepts, rejects (and on what basis), or needs additional time to review.
b. If Gen rejects, Supplier will modify and resubmit the Solutions within 15 days (or as otherwise expressly agreed) to comply with applicable specifications and acceptance criteria. If the Solutions remain non-compliant, Gen may provide its rejection in whole or in part and/or terminate the applicable Order on notice with no further cure period and, in either case, Gen will have no obligation to pay for (and Supplier will promptly refund any amount paid for) the rejected Solutions and other Solutions whose use or value is, in Gen's good faith judgment, materially degraded as a result of the rejected Solutions.

9. Software and SAAS License and Additional Terms. If Solutions include software, whether available on-premise or as a subscription, service or otherwise, (i) Supplier grants Gen and its authorized users a non-exclusive, worldwide, irrevocable, royalty-free, right and license to access and use such software during the term as specified in the applicable Order, (ii) Gen may not (nor permit any third party to): (a) disassemble, decompile, reverse engineer or otherwise attempt to discover the underlying algorithms of any software Solutions, except to the extent permitted by applicable law; or (b) lease, rent or timeshare the software Solutions, and (iii) **Gen's Software and SAAS Terms** attached as **Exhibit C** apply to the software Solutions and are fully incorporated herein.

10. Ownership and License to Pre-Existing Works. As between the parties, and unless otherwise explicitly negotiated and agreed in an Order, (i) Gen owns its Confidential Information which, for clarity, includes Deliverables as defined below, and (ii) Supplier owns its Confidential Information and its products, software, materials, tools, technology and know-how, and all intellectual property rights therein,

that are independently created or obtained by Supplier other than for Gen (collectively, "**Pre-Existing Works**"). For any Pre-Existing Works provided to Gen, and for any Deliverables where ownership does not fully vest with Gen for any reason, Supplier hereby grants Gen a worldwide, royalty free, fully paid, irrevocable right and unrestricted license in and to such Pre-Existing Works and Deliverables for Gen's business purposes, and without accounting or obligation of any kind to Supplier. "**Deliverables**" means all work product and results of services that are created or generated for or on behalf of Gen in the course of providing Solutions to Gen, including without limit all Gen data, information, and content as input, processed and output by any software Solutions and any reports and analysis based thereon and other results that reveal or embody such information.

11. Intellectual Property Assignment. If Supplier is engaged to develop, design, improve, or otherwise work on software, code, or any other technology Solutions or deliverables for or on behalf of Gen, then Supplier agrees to the Intellectual Property Agreement ("**IPA**") attached at **Exhibit D** which terms are fully incorporated herein**.**

12. Warranty. In relation to these Terms and performance hereunder or under any Order, Supplier hereby represents and warrants to Gen all the following:

a. Supplier will comply with applicable laws and regulations including without limit those regarding privacy and personal information, export and import, anti-corruption laws, non-discrimination, the Foreign Corrupt Practices Act, U.K. Bribery Act 2010 and laws of the U.S. Department of the Treasury, Office of Foreign Assets Control; and will further obtain and maintain in effect all required licenses, permits, authorizations and consents to perform under these Terms and each Order and to provide Solutions, Deliverables, and information to Gen.
b. Supplier will conduct its business in an ethical, professional and workmanlike manner consistent with, and no less strict than, the Gen Code of Conduct available at https://www.nortonlifelock.com/legal/code-conduct.
c. Supplier will cooperate with Gen Personnel as reasonably requested by Gen's project contacts designated within the Order or Gen's Procurement organization.
d. Solutions that are not subject to Section 8 (Acceptance) will comply with Supplier's published documentation and with any additional specifications under each Order. For such Solutions that do not comply, Supplier will at its sole cost and expense, and at Gen's option: (i) promptly modify or replace the Solutions to be compliant; or (ii) refund the relevant fees paid for such deficient Solutions and other Solutions whose use or value to Gen is materially degraded as a result of the non-compliant Solutions.
e. Supplier will not provide any software Solutions without first using at least commercially reasonable tools and practices to detect, remove and destroy viruses, trojan horses, back-doors, spyware and other malicious or harmful code, and confirm such removal and destruction.

13. Insurance. Supplier will maintain and comply with the Gen Insurance Requirements specified at attached as **Exhibit E**.

14. Indemnity.
a. Supplier will defend, indemnify and hold Gen and its employees, officers and directors harmless from and against any third party claims, actions or determinations (and resulting damages, costs, expenses, reasonable attorneys' fees and court costs) that (i) any Solutions infringe or misappropriate the intellectual property rights of a third party, (ii) arise from Supplier's breach of Section 3 (Confidentiality), Section 5 (Data Security) or the DPA, or (iii) a relationship other than independent contractor was established between Gen and Supplier or Supplier's Personnel including without limit any claim under the Transfer of Undertakings (Protection of Employees) Regulations 2006, or under the Acquired Rights Directive or other broadly similar legislation.
b. Gen will (i) notify Supplier in a timely manner of any indemnifiable claim, (ii) grant Supplier control of the defense and settlement of the claim and (iii) provide Supplier with reasonable assistance and information as reasonably needed for Supplier to fulfill its obligations hereunder. Supplier will engage reputable reasonably skilled legal counsel in the defense of claims and may not obligate or make an admission on behalf of an indemnified party without the indemnified party's express written consent.
c. If use of Solutions is enjoined due to an infringement claim, Supplier will at its expense promptly take at least one of the following actions: (i) obtain the right for Gen to continue using the Solutions under these Terms; or (ii) replace or modify the infringing Solutions to be non-infringing and substantially equivalent in function, performance, and security as the enjoined Solutions. If neither option can be accomplished despite reasonable efforts, Supplier may terminate Gen's rights and payment obligations hereunder with respect to such Solutions, and Supplier will refund to Gen amounts paid by Gen in connection with the Solutions and any other Solutions whose use or value to Gen is materially degraded as a result of such termination. Gen will have a reasonable time to cease use of replaced/terminated Solutions.

15. LIMIT OF LIABILITY. NEITHER PARTY WILL BE LIABLE UNDER OR IN RELATION TO THESE TERMS FOR ANY (I) AMOUNTS IN EXCESS OF THE AMOUNTS PAID BY OR PAYABLE BY GEN TO SUPPLIER IN THE TWELVE MONTH PERIOD PRECEDING THE EVENTS GIVING RISE TO THE LIABILITY, (II) SPECIAL, INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; OR (III) LOSS OF PROFITS, BUSINESS, REVENUES OR GOODWILL, OR WASTED MANAGEMENT AND STAFF TIME. THE FOREGOING LIMITS AND EXCLUSIONS WILL NOT APPLY TO OBLIGATIONS UNDER OR BREACHES OF SECTION 3 (CONFIDENTIALITY) OR SECTION 14 (INDEMNITY), OR TO EITHER PARTY'S LIABILITY FOR WILLFUL MISCONDUCT OR FRAUD, OR TO DEATH OR PERSONAL INJURY CAUSED BY A PARTY.

16. Notices. Notices to Gen will be sent to vendormanagement@gendigital.com, with a copy to security@gendigital.com in the event of a known or suspected breach of Personal Data. In addition, notices regarding breach or termination will be sent to legal.department@gendigital.com. Notices to Supplier will be sent to its designated contacts as provided to Gen in Supplier's supplier profile or otherwise designated as a Supplier Notices contact in an Order. Hardcopy notices must be sent via reputable delivery service with delivery confirmation to Gen at 487 E. Middlefield Road, Mountain View, CA 94043.

17. Governing Law. These Terms are governed exclusively by the respective choice of law and venue specified below, to which the parties hereby consent to without regard to principles of conflicts of law and hereby waive objections to personal jurisdiction therein. The English language version of these Terms will prevail in the event of any translations. Supplier waives any right to have these Terms officially written in the language of any other applicable country.

- If the contracting Gen party is in the Americas: The laws of California, USA govern with venue in Santa Clara County, California
- If the contracting Gen party is in Europe, the Middle East or Africa: The laws of Ireland govern with venue in Dublin, Ireland
- If the contracting Gen party is in Japan: The laws of Japan govern with venue in Tokyo, Japan
- If the contracting Gen party is in the Asia Pacific region or Australia: The laws of Singapore govern with venue in Singapore

18. Termination.

a. Supplier may terminate these Terms on 30 days' notice if no Orders are active or in effect. Supplier may terminate any Order if Gen has materially breached such Order and failed to cure within 30 days following written notice by Supplier reasonably detailing the breach.

b. Gen may terminate these Terms, any Order(s), and/or purchase order(s) in whole or part on written notice to Supplier, without or without cause, in which case Gen will remain obligated to pay for only those accepted Solutions provided up to the date of termination. If Gen terminates any subscription-based Solutions without cause, Gen will not be entitled to a refund or credit of pre-paid subscription fees for the then-current annual term (or shorter term as may be provided in the appliable Order).

c. Termination of these Terms by either party shall result in termination of all Orders issued under these Terms.

d. On termination of these Terms or any Order by either party, Supplier will (i) at no charge either deliver all Gen Confidential Information and Deliverables to Gen in a reasonable format within 10 business days and/or make Gen Confidential Information and Deliverables available for Gen's retrieval through reasonable means, including without limit through the use of Supplier's tools, for a period of at least 60 days, and (ii) as requested by Gen, and without limiting (i) above, provide additional transition assistance at rates as agreed in good faith by the parties.

19. Trade Compliance. Each party will comply with export laws and regulations applicable to such party. Supplier shall not export or re-export, or request Gen to export or re-export, any Solutions, including all Solutions and/or technical data received from Gen or any direct product thereof, directly or indirectly, to any country, entity or person prohibited by the U.S. Government. Supplier acknowledges that compliance with U.S. export laws may cause delays in shipments and/or prohibit Supplier from exporting certain Solutions to certain countries and entities for certain uses. In no event shall Gen be liable for any such delays or prohibition.

20. Verification. Upon Supplier's request or inquiry regarding Gen's use of Solutions, which may not occur more than once in any twelve-month period, Gen will conduct an internal effort to verify its use of Solutions in accordance with purchased quantities and other entitlements. If Gen's actual use exceeded purchased quantities and other entitlements, Gen may cease the excess use at no cost or purchase appropriate quantities at the rates or per-unit fees previously paid by Gen for the relevant Solutions (or discount equivalent if not like-for-like Solutions). No other fees, penalties or retroactive amounts will be due and Gen shall not be deemed to have infringed or misappropriated any intellectual property rights or to have otherwise breached these Terms. Any additional verification or audit effort will be performed if and as agreed in good faith by the parties at such time, and under additional terms of confidentiality specific to the effort.

21. Miscellaneous. Notwithstanding anything to the contrary:

a. The parties are independent contractors engaged on a non-exclusive basis. Neither party has authority to bind or make any representation, warranty, or commitment on behalf of the other party.

b. These Terms, along with terms incorporated herein by reference and each Order, comprise the entire agreement and understanding between the parties regarding the subject matter herein. No other terms, quotes, agreements, or understandings between the parties shall be valid or enforceable unless agreed to in the form of a mutually executed amendment to these Terms or change order to an Order. Notwithstanding the preceding, Gen may, from time to time, modify these Terms, provided that the terms in effect on the effective date of an Order shall continue to govern only that particular Order.

c. These Terms will supersede and control in the event of any conflict or inconsistency with the terms of any Order, including without limit any conflicting order of precedence provisions and any Supplier terms incorporated into such Order by URL or other reference. In the event of any conflict or inconsistency between these Terms and any Order, these Terms will control.

d. Neither party may transfer, novate, or assign these Terms without the other party's express written consent, except to their respective affiliates, and to their successors in the event of merger, acquisition, or asset sale. All other attempts to transfer, novate or assign shall be deemed to be null and void. If Supplier assigns these Terms or any Order to a competitor of Gen that is named in its then-most recent 10-K SEC filing, Gen may terminate these Terms and any Order on written notice.

e. If any provision of these Terms is found to be illegal or unenforceable in whole or in part, such provision shall be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of these Terms shall remain in full force and effect.
f. The provisions of these Terms which, by their nature, are on-going will survive termination of these Terms, for example and without limit confidentiality, ownership, indemnification, limit of liability, and this Section 21 (Miscellaneous).
g. The parties agree that these Terms are agreed between sophisticated parties and thus any principle of construction, legal doctrine or rule of law that provides for construction against the drafter under any circumstance, shall not apply to these Terms.
h. A party's failure or delay to exercise any right or require performance under these Terms or any Order shall not be deemed a waiver of any further such right or performance.
i. Gen is a participant in the United Nations Global Compact ("**Global Compact**"), an international initiative working to advance ten universal principles in the areas of human rights, local labor laws, environmental and anti-corruption. Gen encourages Supplier to conduct its business pursuant to the Global Compact's Ten Principles at https://www.unglobalcompact.org/what-is-gc/mission/principles. Visit www.unglobalcompact.org for more information.
j. **Gen's Delivery Terms** located at www.nortonlifelock.com/us/en/procurement/delivery-terms/ are fully incorporated herein and apply to Solutions that are physically delivered to Gen.
k. Except as expressly provided under the Standard Contractual Clauses to the DPA there are no third-party beneficiaries to these Terms or any Order.

Exhibit A
Data Processing Agreement (DPA)

This Data Processing Agreement (**"DPA"**) is made between Gen Digital Inc. and its affiliates as identified in any Order (**"Gen"**) and the seller or provider of any Solutions as identified in such Order (**"Provider"**).

Gen and Provider are each a **"Party"** or the **"Parties"** to this DPA.

WHEREAS in this context:

Gen has procured from Provider certain products and/or services under the Gen Procurement Terms and Conditions and/or Order (the **"MPA"**) that requires the processing of Personal Data. This DPA is supplemental to the MPA and sets out the terms that apply to the extent that the Provider Processes or causes to be Processed any Personal Data.

The Parties agree as follows:

1. **Definitions**. Capitalized terms used in this DPA and not otherwise defined in this DPA will shall have the meaning as ascribed to them in the MPA. If any definitions in the MPA or this DPA conflict with statutory definitions provided in any Data Protection Law, the definition in the applicable Data Protection Law shall control.

   "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the thresholds set out in the CCPA.

   "California Personal Data" means the Gen Personal Data the Processing of which is subject to the CCPA.

   "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 es seq., as amended, in particular, by the California Privacy Rights Act of 2020.

   "Controller" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

   "Data Protection Law" means the EU Data Protection Law, the CCPA, the UK GDPR, the Swiss Data Protection Law and any other data protection laws which may be applicable to the Personal Data Processed under the MPA.

   "Deidentified Information" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the Business that possesses the information: (i) takes reasonable measures to ensure that the information cannot be associated with a consumer or household, (ii) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision, and (iii) contractually obligates any recipients of the information to comply with all provisions under the CPPA and Section 11.6 of this DPA.

   "EEA" means the European Economic Area.

   "EU Data Protection Law" means (i) the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data for the transfer of personal data to a third country (**"GDPR"**) and (ii) any applicable data protection laws of any EEA member state.

   "EU Personal Data" means the Gen Personal Data the Processing of which is subject to the EU Data Protection Law.

   "Gen Personal Data" means Personal Data that the Provider Processes under the MPA.

"Personal Data" means any information related to any identified or identifiable natural person ("**Data Subject**"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, or as defined by the Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

"Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means a natural or legal person, public authority, agency, or other body which Processes personal data on behalf of the Controller.

"**Service Provider**" means a person that processes personal information on behalf of a Business that receives from or on behalf of the Business a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract meets the requirements of the CCPA.

"Services" means the services as described in MPA.

"Standard Contractual Clauses" are as defined in Section 10.2 of this DPA.

"**Swiss Data Protection Law**" means the Swiss Federal Act on Data Protection.

"**Swiss Personal Data**" means the Gen Personal Data the Processing of which is subject to the Swiss Data Protection Law.

"**UK GDPR**" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data for the transfer of personal data to a third country as it forms part of the law of England and Wales.

"**UK Personal Data**" means the Gen Personal Data the Processing of which is subject to the UK GDPR.

2. <u>Subject of the DPA</u>

a. With respect to Processing of Gen Personal Data in connection with the MPA, Gen shall act as the Controller and Provider as the Processor.

b. Detailed specification of Gen Personal Data Processed, including the subject-matter, the nature and purpose of the Processing, the type of personal data and categories of data subjects are provided in the Order.

c. The subject-matter of the Processing of Personal Data is the provision of Services under the MPA.

d. The nature of the Processing of Personal data may include but is not limited to: collection, recording, organization, storage, use, disclosure, erasure, augmentation, enrichment and transmission in connection with provision of the Services.

3. <u>Compliance with Laws and Processing Instructions</u>.

a. Each Party will comply with the Data Protection Law as applicable to it. To the extent required by any Data Protection Law, the Parties agree to negotiate in good faith and execute any such additional, supplemental or revised documents pertaining to the Processing of Gen Personal Data as reasonably necessary for the provision of Services under the MPA.

b. The Provider shall Process the Gen Personal Data only on documented instructions from Gen, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so under applicable Data Protection Law; in such case, the Provider shall inform Gen of that legal requirement before Processing of the Gen Personal Data, unless that law prohibits such information on important grounds of public interest. Provider shall immediately inform Gen if, in its opinion, an instruction infringes on any Data Protection Law.

c. Provider shall Process Gen Personal Data solely for the purposes set out in the MPA and cannot Process Gen Personal Data for any other purposes to be determined by the Provider.

d. With respect to Processing of Gen Personal Data, the Provider may only use such employees, members of its corporate bodies or other similar persons who are sufficiently trained, familiar with all the Gen's instructions and Provider's internal guidelines.

e. The Provider shall Process Gen Personal Data for as long as it is necessary to fulfill its obligations under Gen´s instructions. After the termination or expiry of the MPA, the Provider shall, without undue delay, destroy or remove all Gen Personal Data that it has not returned Gen. This does not apply if the Provider has legitimate reasons to further Process Gen Personal Data under Data Protection Law.

4. Security

a. The Provider hereby represents and warrants to Gen that it has implemented appropriate technical and organizational measures to ensure the security of the Gen Personal Data, including protection against a breach of security leading to a Personal Data Breach. In particular, the Provider hereby represents and warrants that it has, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including (i) internal policies and practices for protection of Personal Data, including for training and supervision of its staff, especially where cross-border transfers and Processing are concerned, and (ii) the technical and organizational measures explicitly specified in the MPA. The Provider shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The Provider shall encrypt the Gen Personal Data and shall (i) keep the encryption key separately from the Gen Personal Data and (ii) not provide to any public authority an encryption key to the Gen Personal Data or assist the public authority in any other way in obtaining the Gen Personal Data, unless required to do so by applicable law.

c. The Provider shall grant access to the Gen Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the MPA. It shall ensure that persons authorized to Process the Gen Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Personal Data Breach Notification and Remediation.

a. Provider will promptly, but not later than 24 hours from becoming aware of the Personal Data Breach, notify Gen of the occurrence or possible occurrence of the Personal Data Breach affecting Gen Personal Data. Provider shall send all notifications of Personal Data Breaches to: security@gendigital.com. Such notification shall contain, at least: (i) description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned); (ii) its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects; and (iii) the details of a contact point where more information concerning the Personal Data Breach can be obtained.

b. In case of the Personal Data Breach, the Provider shall provide reasonable cooperation to Gen in informing the affected Data Subjects.

c. Except and only to the extent expressly required by law, Provider agrees that it will not inform any third party that Gen Personal Data has been involved in a Personal Data Breach without Gen's prior written consent. If Provider is compelled by law to provide public/third-party notification of a Personal Data Breach, Provider will not identity Gen (directly or indirectly) and will use commercially reasonable efforts to obtain Gen's prior approval regarding the content of such disclosure to minimize any adverse impact to Gen, and its respective customers and/or employees.

6. Processing carried out by other persons

a. Gen generally authorizes the Provider to engage other Processors (sub-processors) listed in the Order. The Provider shall inform Gen of any intended changes concerning the addition or replacement of sub-processors together with the information necessary for Gen to assess the sub-processor in question without undue delay (at least 30 business days prior to the engagement of the sub-processor in question), thereby giving Gen the opportunity to object to such changes. If Gen does not object to changes in

sub-processors within 30 business days of the receipt of the notification of change, the change is considered as approved. A list of sub-processors approved by Gen as at the date of this DPA is included in the Order.

b. In relation to the Processing of Gen Personal Data, the sub-processors shall maintain confidentiality, i.e. they shall not disclose the Gen Personal Data or make it available to any other person without Gen's consent. This does not apply to the legal obligation to disclose Personal Data to entities authorized to receive such data by law. The confidentiality obligation is not limited and shall apply even after termination of the MPA.

c. The Provider shall ensure by way of a contract that sub-processors comply with the obligations to which the Provider is subject pursuant to the DPA and under Data Protection Law. At Gen's request, the Provider shall provide a copy of its sub-processor agreements and any subsequent amendments to Gen. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Provider may redact the text of the sub-processor agreements prior to sharing the copy.

d. The Provider shall remain fully responsible to Gen for the performance of the sub-processor's obligations in accordance with the DPA. The Provider shall notify Gen, without undue delay, of any failure by the sub-processor to fulfil its contractual obligations.

e. The Provider shall agree a third party beneficiary clause with the sub-processor whereby - in the event the Provider has factually disappeared, ceased to exist in law or has become insolvent - Gen shall have the right to terminate the sub-processor agreement and to instruct the sub-processor to erase or return the Gen Personal Data.

7. Cooperation and assistance

a. The Provider shall deal promptly and adequately with inquiries from Gen about the Processing of Gen Personal Data in accordance with this DPA and provide Gen with the necessary assistance to comply with the applicable Data Protection Law, in particular:
   i. with the handling of Data Subjects´ requests; and
   ii. when carrying out data protection impact assessment and consulting with the data protection authorities.

b. In case the Provider receives a Data Subjects´ request relating to the Gen Personal Data Processed under the MPA, the Provider shall promptly, but not later than within two business days, forward such request to Gen. The Provider shall not respond to such a request without Gen's prior written consent.

8. Control and audit

a. The Provider is obliged to allow Gen to check the Provider's compliance with all obligations under this DPA and Data Protection Law.

b. The Provider shall upon Gen´s request, without undue delay, submit documents proving that the Provider Processes Gen Personal Data in accordance with this DPA and Data Protection Law and enable the audit to be carried out by Gen or a person authorized by it to perform it. Gen shall notify the Provider about its intent to perform an audit reasonably in advance.

c. If a control or an audit is carried out at the Provider´s place by public authorities, the Provider shall immediately notify Gen about such control or audit and provide relevant documents, unless prohibited from doing so under applicable law.

9. International Transfers of Personal Data

Provider and its sub-processors shall only transfer Gen Personal Data from its country of origin in accordance with the Data Protection Law.

10. Additional Provisions Applicable to the EU Personal Data

a. The provisions set out in this Section 10 shall only apply to Processing of the EU Personal Data.

b. Any transfer of EU Personal Data by the Provider to a third country (in the sense of the GDPR) shall be governed by the standard contractual clauses attached as Schedule 1 to this DPA (the **"Standard Contractual Clauses"**).

c. The Provider confirms that it is not an electronic communication service provider pursuant to the US Foreign Intelligence Surveillance Amendments Act of 2008 **("FISA"**) or subject to any other similar legislation of any country outside the EEA that imposes requirements for disclosure of Personal Data to public authorities or grants such public authorities powers of access to Personal Data (for example, for criminal law enforcement purposes, regulatory oversight or national security) which restrict the fundamental rights of Data Subjects (including by failing to provide adequate redress by a judicial or other independent authority) and which go beyond what is necessary and proportionate in a democratic society to secure important legitimate aims such as such those listed in Article 23 (1) of the GDPR (defense, combating criminal and other unlawful activities, etc.).

d. The Provider confirms that, in the last three years before the execution of the MPA, it has not disclosed to any public authority any Personal Data required by this public authority for national security reasons, including under Section 702 of the FISA.

11. <u>Additional Provisions Applicable to the California Personal Data</u>

a. The provisions set out in this Section 11 shall only apply to Processing of the California Personal Data.

b. **Roles and Scope.**

i. This DPA applies only to the collection, retention, use, disclosure, and sale or sharing, as the case may be, of Personal Data provided by Gen to, or which is Collected on behalf of Gen by, Provider to provide Services to Gen pursuant to the MPA or to perform a business purpose.
ii. The Parties acknowledge and agree that Gen is a Business and appoints Provider as a Service Provider to Process Personal Data on its behalf and at its direction.

c. **Restrictions on Processing.** Except as otherwise permitted by the CCPA, Provider is prohibited from:

i. selling or sharing the Personal Data;
ii. retaining, using, or disclosing Personal Data for any purpose, including any commercial purpose, other than for the specific purpose of performing the Services specified in the MPA entered into with Gen, as set out in this DPA;
iii. retaining, using, or disclosing Personal Data outside of the direct business relationship between Provider and Gen; or
iv. Combining the Personal Data that the Provider receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, with the Personal Data received from or on behalf of Gen hereunder.

d. Upon direction by Gen, and in any event no later than 30 days after receipt of a request from Gen, Provider shall promptly delete Personal Data as directed by Gen.

e. Provider shall not be required to delete any Personal Data to comply with a Consumer's request directed by Gen if it is necessary to maintain such information in accordance with the CCPA, in which case Provider shall promptly inform Gen of the exceptions relied upon to retain Personal Data. Provider shall not use Personal Data retained for any other purpose than provided for by that exception.

f. **Deidentified Information.** In the event that any Party shares Deidentified Information with another Party, the receiving Party warrants that it: (i) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (ii) has implemented business processes that specifically prohibit reidentification of the information; (iii) has implemented business processes to prevent inadvertent release of Deidentified Information; and (iv) will make no attempt to reidentify the information.

g. **No Sale of Information.** The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the MPA.

12. <u>Additional Provisions Applicable to UK Personal Data</u>

a. The provisions set out in this Section 12 shall only apply to Processing of the UK Personal Data.

b. Any transfer of the UK Personal Data by the Provider to a third country (in the sense of the UK GDPR) shall be governed by the Standard Contractual Clauses attached as Schedule 1 to this DPA as supplemented by template Addendum B.1.0 issued

by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those mandatory clauses (the **"UK Approved Addendum"**) and Part 1 of the UK Approved Addendum shall be populated as set out below:

- Table 1. The "start date" will be the date this DPA enters into force. The "Parties" are Gen as exporter and the Provider as importer.
- Table 2. The "Addendum EU SCCs" are the modules and clauses of the Standard Contractual Clauses in Commission Implementing Decision (EU) 2021/914, including the text from module two and three of such clauses and not including any clauses marked as optional.
- Table 3. The "Appendix Information" is as set out in this DPA and Order.
- Table 4. The exporter may end the UK Approved Addendum in accordance with its Section 19.

c. In the event that: (1) the UK Approved Addendum is no longer valid for use under Article 46 of the UK GDPR; and (2) the Information Commissioner issues standard data protection clauses under s.119A(1) of the UK Data Protection Act 2018 which incorporate and modify the EU Standard Contractual Clauses to be effective under the laws of the United Kingdom (**"New UK Standard Contractual Clauses"**), then the Parties agree that the New UK Standard Contractual Clauses shall apply to any transfer of the UK Personal Data by the Provider to a third country (in the sense of the UK GDPR) from such date as Gen notifies Provider, with the details of the Parties, Annexes and modules as specified in this DPA in relation to the EU Standard Contractual Clauses. The Parties agree that Gen may, by notice to the Provider, make any further amendments to the application of the New UK Standard Contractual Clauses as Gen deems reasonably necessary to implement such replacement standard contractual clauses.

13. Additional Provisions Applicable to Swiss Personal Data

a. The provisions set out in this Section 13 shall only apply to Processing of the Swiss Personal Data.

b. Any transfer of the Swiss Personal Data by the Provider to a third country (in the sense of the Swiss Data Protection Law) shall be governed by the Standard Contractual Clauses, provided that any references in the Standard Contractual Clauses to the GDPR shall refer to the Swiss Data Protection Law, the term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses, and the clauses shall also protect the data of legal persons.

14. Order of Precedence.

If there is a conflict between the MPA and this DPA, the terms of this DPA will control including the terms of the Standard Contractual Clauses.

Schedule 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to

accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation

available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the laws of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such court

ANNEX I
PARTIES AND DESCRIPTION

A. LIST OF PARTIES

Data exporter(s):

Name, Address and Contact person's name, position and contact details: as set out in the Order.

Activities relevant to the data transferred under these Clauses: The relevant activities of the data exporter are as set out in the MPA.
Role: Controller.

Data importer(s):

Name, Address and Contact person's name, position and contact details: as set out in the Order.

Activities relevant to the data transferred under these Clauses: The relevant activities of the data importer are as set out in the MPA.
Role: Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set out in the Order.

Categories of personal data transferred

As set out in the Order.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set out in the Order.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis

As set out in the Order.

Nature of the processing:

The nature of the processing of personal data may include but is not limited to: collection, recording, organization, storage, use, disclosure, erasure, augmentation, enrichment and transmission in connection with provision of the Services.

Purpose(s) of the data transfer and further processing

The importer will process personal data for the purposes of providing the Services under the MPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The importer shall process personal data for as long as it is necessary to fulfill its obligations under exporter´s instructions. After the termination or expiry of the MPA, the importer shall, without undue delay, destroy or remove all personal data that it has not returned importer. This does not apply if the exporter has legitimate reasons to further process personal data under data protection law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As set out in the Order.

C. COMPETENT SUPERVISORY AUTHORITY

Irish Data Protection Commission

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As set out in the MPA.

ANNEX III
LIST OF SUB-PROCESSORS

As set out in the Order.

Exhibit B
Master Supplier Security Requirements

1. SECURITY REQUIREMENTS

The Supplier shall operate in compliance with: (i) the requirements set forth in this document, (ii) industry best practices and standards; and iii) any applicable legal and regulatory requirements, whichever is the stricter, higher or more protective standard.

Nothing herein is intended or shall be construed to limit any of Supplier's obligations under the Procurement Terms and Conditions or any other agreement or applicable terms between Supplier and Gen ("Terms"). In the event of any conflict between such provisions and this Master Provider Security Requirements, the stricter, higher, or more protective standard shall govern unless otherwise expressly agreed to in writing and signed by both parties.

2. DEFINITIONS

TERM	DEFINITION
Gen Data	Any Gen data, content, and information that Supplier is provided, or has access to.
Gen Restricted Data	Highly sensitive Gen Data limited to very few individuals and shared only on a need-to-know basis. Applies to Gen Data that must be protected due to legal or regulatory requirements; may give Gen a competitive advantage. Any Gen Data containing Nonpublic Personal Information (NPI), Personally Identifiable Information (PII), or Protected Health Information (PHI) is considered Gen Restricted Data. Unauthorized disclosure impact will be severe. Unauthorized access, use, or disclosure is expected to have a major reputational, regulatory, or financial impact. The business impact of loss or modification will be severe and is expected to have a major adverse effect on operations, assets, or individuals.
Gen Confidential Data	Sensitive Gen Data limited to small groups (e.g., project teams) and shared only on a need-to-know basis. Applies to company secrets, proprietary code, and other data that would give Gen a competitive advantage. Any Gen Data that is not expressly classified under this Section 2 as either Gen Restricted Data, or Internal Use Only is Gen Confidential Data. Unauthorized disclosure impact will be severe to moderate. Unauthorized access, use, or disclosure may have a major reputational or financial impact but is not expected to have a regulatory impact. The business impact of loss or modification will be severe to moderate and may have a major adverse effect on operations, assets, or individuals.
Gen Internal Use Only	Non-sensitive Gen Data used for conducting company business. Applies to data commonly available within Gen and used for daily operations. Unauthorized disclosure impact will be minimal. Unauthorized access, use, or disclosure is not expected to have a reputational, regulatory, or financial impact. The business impact of loss or modification will be minimal and may have a limited adverse effect on operations, assets, or individuals.

TERM	DEFINITION
Handle (or "handle")	Any processing operation(s) performed upon Gen Data, whether by automatic means or not, such as collecting, recording, using, accessing, copying, reproducing, retaining, storing, disclosing, modifying, altering, transferring, transmitting, deleting, destroying or otherwise disposing of, selling, assigning, licensing, or marketing.
Personnel	Supplier's employees, contractors, subcontractors, and/or third parties engaged by or on behalf of Supplier that provide services to Gen and/or handle Gen information.
Gen Information Assets	Gen assets including end user computing devices, networks, infrastructure, data repositories.

3. INFORMATION SECURITY POLICIES

3.1. Management Direction for Information Security

3.1.1. Supplier shall maintain an Information Security Policy (ISP) that is reviewed and approved at least annually at the executive level. Supplier shall ensure that all Personnel have access and comply with the ISP.

4. ORGANIZATION OF INFORMATION SECURITY

4.1. Internal Organization

4.1.1. Supplier shall adopt physical, technical and organizational security measures in accordance with industry best practices and standards and be in compliance with all applicable legal and regulatory requirements as they apply to the Supplier's services being provided to Gen.

5. HUMAN RESOURCE SECURITY

5.1. Prior to employment

5.1.1. Supplier shall, when and to the extent legally permissible, perform background verification checks in compliance with the Gen policies for all Personnel who may have access to Gen Restricted Data or Gen Confidential Data and/or Gen Information Assets. Such background checks shall be carried out in accordance with and as permitted under applicable regulation and law and shall include the following regional equivalent items: SSN Trace, Global Blacklist Search, Criminal County Search (5-Year Address History), Criminal Federal Search (5-Year Address History), and Financial Sanctions Search.

5.2. During employment

5.2.1. Supplier shall provide security awareness training based on industry best practices and standards to all Personnel at least annually.

5.2.2. Additional Training

5.2.3. Supplier shall complete and implement additional training as may be required by Gen from time to time.

5.3. Termination and change of employment

5.3.1. Supplier shall implement effective user termination / transfer controls that include access removal / disablement immediately upon termination or transfer of Personnel or when such Personnel no longer require handling of Gen Data as part of their job duties for Supplier.

6. ASSET MANAGEMENT

6.1. Responsibility for assets

6.1.1. Suppliers that use Gen Information Assets shall strictly adhere to the most current version of Gen's Acceptable Use Standard.

6.1.2. Gen Information Assets may not be modified in any way or used to provide services to any other parties other than by prior express written agreement with Gen.

6.2. Media handling

6.2.1. Destruction Requirements and Compliance Evidence

6.2.1.1. Any and all Gen Data is and shall remain the sole property of Gen, and Supplier shall not acquire any rights or licenses therein except as expressly set forth in the relevant Terms. Supplier shall return to Gen (or at Gen's option, destroy) any and all Gen Data and any other information and materials that contain such Gen Data (including all copies in any form) immediately upon Gen's request, or upon the earlier of the completion of services or termination of the relevant Terms.

6.2.1.2. Supplier shall ensure secure disposal of systems and media to render all Gen Data contained therein as undecipherable or unrecoverable prior to final disposal or release from Supplier's possession. This shall be undertaken in accordance with U.S. National Institute of Standards and Technology (NIST) approved standards and within ten (10) days following Gen's request, Supplier shall provide Gen with a written certificate of destruction.

6.2.2. Removable Media

6.2.2.1. Use of removable media is prohibited. All ports for USB and external drives must be disabled on all workstations that handle Gen Data.

7. ACCESS CONTROL

7.1. Business requirements of access control

7.1.1. Supplier shall implement strong access control and restrict access to operating system configurations to authorized, privileged personnel for systems handling Gen Restricted Data or Gen Confidential Data.

7.1.2. Mobile devices and teleworking

7.1.2.1. Supplier shall require that all Personnel who are able to access to Gen Data must use a Supplier issued device, excluding mobile devices.

7.1.2.2. Supplier shall not allow (and shall restrict) Personnel to access Gen Data via a mobile device.

7.1.3. User access management

7.1.3.1. Supplier shall ensure that the Supplier's system (network, hosting and application) is designed in compliance with the least privilege principle.

7.1.3.2. Supplier shall enforce the use of strong passwords for all Supplier systems (network, hosting, and application) as follows:

- Passwords are at least ten (10) characters long;
- Contain at least three of the following: Upper-case letters, lower-case letters, numbers, non-alphabetic characters;
- Expire after 90 days for all systems; and
- Are never hard-coded, stored in files, or stored or transmitted in clear text

7.1.3.3. All vendor default passwords within software and hardware products must be changed before or during installation

7.1.4. User responsibilities

7.1.4.1. For administrative accounts and for any accounts that allow remote access to systems, Supplier shall use multi-factor authentication or other positive controls such as increased password length, shorter password life or restrictive white lists of users to restrict access to administrative accounts.

7.1.5. System and application access control

7.1.5.1. Supplier shall maintain documentation on the applicable application, architecture, process flows and/or data flow diagram, and security features for applications handling Gen Restricted Data or Gen Confidential Data.

8. CRYPTOGRAPHY

8.1. Cryptographic controls

8.1.1. Supplier shall use NIST or PCI approved encryption and hashing standards (e.g. SSH, SSL, TLS) for transmission and storage of Gen Restricted Data and Gen Confidential Data.

8.1.1.1. Where necessary to be stored on a portable device, the device shall be protected by full disk encryption.

8.1.2. Gen Restricted Data or Gen Confidential Data stored on archive or backup systems shall be subject to at least the same protection measures used in the live environment.

9. PHYSICAL AND ENVIRONMENT SECURITY

9.1. Secure areas

9.1.1. Supplier shall ensure the physical and environmental security of all areas containing Gen Restricted Data or Gen Confidential Data, including but not limited to data centers and server room facilities, are designed to:

9.1.1.1. Protect information assets from unauthorized physical and logical access based on role, duties, grade level, geographical location for all Personnel.

9.1.1.2. Manage, monitor, and log movement of Personnel into and out of such facilities and all other applicable areas including, but not limited to, badge access control, locked cages, secure perimeter, cameras, monitored alarms, and enforced use provisioning controls, when and to the extent legally permissible.

9.1.1.3. Guard against environmental hazards such as heat, fire and water damage.

9.1.1.4. Security Personnel deployed to supervise the access to premises, and strict policies to ensure Gen Data is not removed from the premises.

9.1.2. In regards to the data centers, contact centers and server facilities, Supplier shall logicaly or physically segregate Gen Data from other customer or tenant's data.

10. OPERATIONS SECURITY

10.1. Operational procedures and responsibilities

10.1.1. Supplier shall implement operating system hardening for hosts and infrastructure handling Gen Restricted Data or Gen Confidential Data. Operating system hardening includes, but is not limited to, the following configurations and practices:

- Strong password authentication, at least as secure as set out in Section 7.1.3.2 above.
- Inactivity time-out
- Disabling unused ports/services
- Log management
- Disabling or removal of unnecessary or expired accounts
- Changing default account passwords and where possible default account names
- Timely patching and updates to firmware, OS and system, application and database level software

10.2. Protection from malware

10.2.1. Supplier shall employ and maintain comprehensive anti-malware solutions configured to download signatures at least daily and a firewall solution (or other threat protection technologies) for end user computing devices which connect to the Gen network or handle Gen Restricted Data or Gen Confidential Data.

10.2.2. Supplier shall prohibit and disable the use of external devices for storing or carrying, or in use with machines handling Gen Restricted Data or Gen Confidential Data. External devices include without limit: flash drives, CDs, DVD, external hard drives and other mobile devices.

10.3. Logging and Monitoring

10.3.1. Supplier shall ensure system audit or event logging and related monitoring procedures are implemented and maintained to proactively record user access and system activity for routine review. All log files shall be retained for at least twelve (12) months and access restricted to authorized personnel only.

10.3.2. Suppliers who have physical access to Gen Restricted Data or Confidential Data shall maintain logs for all entry points from CCTV, badge readers and sign-in sheets. All log files shall be retained for at least twelve (12) months and access restricted to authorized Personnel only, unless appliable data protection laws require a shorter retention period.

10.4. Vulnerability Scanning

10.4.1. Suppliers who handle Gen Restricted Data or Gen Confidential Data, or host internet accessible sites on behalf of Gen (either directly or through third parties), shall:

10.4.1.1. Utilize industry standard scanning tools to identify network, host and application vulnerabilities.

10.4.1.2. Perform at least monthly internal vulnerability scans of network(s), host(s) and application(s).

10.4.1.3. Perform ad-hoc vulnerability scanning to identify network, host, and application vulnerabilities prior to release to production and after more than minor changes.

10.4.1.4. Remediate all critical, high and medium vulnerabilities according to CVSS scoring, prior to release to production and thereafter according to the following vulnerability remediation timeframes:

- Critical/High – 30 days
- Medium – 60 days
- Low – 90 days or prior to the next testing time period

10.4.1.5. For critical zero-day vulnerabilities, recommended remedial risk mitigation actions are implemented without undue delay in no event later than the timeframe specified for critical vulnerabilities in this section. Supplier shall promptly implement recommended remedial risk mitigation action, such as applying a software patch, software upgrades, application configuration modifications, or other compensating security preventative control methods, no later than twelve (12) business days after the recommended remedial action has been published, tested and determined safe for installation and use.

10.5. Penetration Testing

10.5.1. Suppliers who handle Gen Restricted Data or Gen Confidential Data, or have access to the Gen network shall:

10.5.1.1. Utilize an independent third-party to perform an at least annual penetration test of network(s), host(s) and application(s).

10.5.1.2. Utilize an independent third-party to perform ad-hoc penetration tests prior to release to production and no less than thirty (30) days after significant changes.

10.5.1.3. Remediate all critical, high and medium vulnerabilities discovered by the pen-tester , prior to release to production and thereafter according to the following vulnerability remediation timeframes:

- Critical/High – 30 days
- Medium – 60 days
- Low – 90 days (or prior to the next testing time period

10.5.1.4. Provide to Gen the executive summary portion of the third party penetration test relating to the network(s), host(s) and application(s).

10.5.1.5. Review the penetration test reports for any appointed subcontractor or fourth party to Gen, who handles Gen Restricted Data or Gen Confidential Data, or hosts internet accessible sites for Supplier on behalf of Gen and notify Gen of their use.

10.5.1.6. Gen reserves the right to independently or utilize an authorized third-party to perform a network penetration test on the area(s) of the Supplier's network that handles Gen Restricted Data or Gen Confidential Data, connects to the Gen network, or hosts internet accessible sites on behalf of Gen.

11. COMMUNICATIONS SECURITY

11.1. Network-Level Requirements

11.1.1. Supplier shall use firewall(s) to protect networks that handles Gen Restricted Data or Gen Confidential Data or host internet accessible sites on behalf of Gen. The firewall(s) shall be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Supplier shall have network-based security monitoring (i.e., syslog, security information and event management (SIEM) software or host-based intrusion detection systems) for the segment(s) which handles Gen Restricted Data or Gen Confidential Data.

11.1.2. Supplier is not permitted to use a dynamic DNS service for their external facing website IP address. If a static IP address cannot be provided, then a non-internet-based method of interaction/communication shall be used.

11.2. Hosting-Level Requirements

11.2.1. The Supplier shall not use or change a cloud environment in any capacity (i.e., IaaS, PaaS, SaaS, process, transmit, access and store data) without obtaining express prior written consent from Gen. If Gen provides such permission, the Supplier shall logically segregate all Gen Restricted Data and Confidential Data.

11.3. Information transfer

11.3.1. For data originating from a Gen U.S. entity: Supplier shall not access, store, process and/or use any Gen Data in a location outside the United States without Gen's prior explicit approval. Additionally, Supplier shall ensure that all Personnel who have access to Gen Data are located in the United States. If access or handling is performed outside of the United States additional terms or agreements may be appropriate and Supplier agrees to promptly and in good faith enter into such additional terms or agreements as Gen may require from time to time.

11.3.2. For data orignating from a Gen EU entity or otherwise governed under EU and UK data protection laws: Supplier shall not access, store, process and/or use any Gen Data in a location outside the European Union without Gen's prior explicit

approval. Additionally, Supplier shall ensure that all Personnel who have access to Gen Data are located in the European Union. If access or handling is performed outside of the European Union additional terms or agreements may be appropriate and Supplier agrees to promptly and in good faith enter into such additional terms or agreements as Gen may require from time to time.

12. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

12.1. Security in development and support processes

12.1.1. Suppliers that develop source code for Gen, handle Gen source code (including without limit any Gen product or service source code), or develop and maintain applications that handle Gen Restricted Data or Gen Confidential Data shall:

12.1.1.1. Deliver at least annual secure code training to all Personnel in-scope for delivering such services to Gen. Developers shall be proficient in the OWASP Top 10 and the CWE/SANS Top 25 vulnerabilities and their appropriate remediation techniques. Supplier shall provide Gen with this initial evidence of compliance within thirty (30) days from the effective date of the relevant Terms between Gen and Supplier and annually thereafter.

12.1.1.2. Maintain and evidence an annual review of a documented change management process and software development lifecycle (SDLC), which includes:

- Independent secure code reviews;
- Secure programming guidelines and protocols for developing applications;
- Threat model methodology to identify the key risks to applications and/or source code; and
- Application security testing (testing may include static application security testing (SAST), dynamic application security testing (DAST) and third-party penetration testing)

12.2. Test Data

12.2.1. Supplier may never use Gen Data for any testing scenarios.

13. SUPPLIER RELATIONSHIPS

13.1. Information security in supplier relationships

13.1.1. Suppliers that either connect to any Gen network, handle Gen Restricted Data or Gen Confidential Data and/or develop or host internet assessable sites on behalf of Gen, shall ensure that they maintain an applicable SOC 2 Type 2 attestation and/or, ISO/IEC27001 certification. Supplier shall provide Gen with a copy of the SOC 2 Type 2 report, and/or ISO27001 Statement of Applicability with certificate.

13.1.2. Suppliers who cannot provide an applicable attestation or certification as stated above, are required to undertake a Gen's security risk assessment (SRA) or provide a SIG LITE as requested by Gen on an annual basis.

13.1.3. Gen is a PCI Level 1 merchant. Any Supplier who handles credit card data on behalf of Gen, shall at all times remain in compliance with the most recent version of Payment Card Industry Data Security Standard (PCI DSS) to the extent PCI DSS is applicable to the services provided under the Terms (e.g., if Supplier accesses, collects, uses, retains, processes, discloses or transfers any cardholder data as defined under PCI DSS or any other data protected or subject to PCI DSS (collectively, "PCI Data"), or if any part of such services impacts the security of the PCI Data environment). Upon request by Gen, Supplier shall promptly provide sufficient proof, as determined by Gen in its sole discretion, of compliance with PCI-DSS to Gen. If Supplier has knowledge of a potential violation of PCI DSS, Supplier shall notify Gen promptly, but no later than 48 hours or a shorter priod where required under PCI DSS, after obtaining such knowledge and come into compliance with PCI DSS within the time frame specified by Gen, but no later than 30 days, after Supplier obtains knowledge of such violation. Supplier shall ensure that all of its Personnel comply with the same obligations that apply to Supplier under the Terms and remain liable to Gen for compliance with the Terms by its Personnel. Supplier shall provide Gen with this initial evidence of compliance (PCI AoC) within thirty (30) days from the effective date of the relevant Terms between Gen and Supplier and annually thereafter.

13.1.4. Where Supplier or its Personnel have a reasonable belief that Gen Data may have been compromised, including without limit any unauthorized handling, Supplier shall notify Gen thereof without undue delay after becoming aware, and Gen may conduct an SRA on three (3) days' notice at the Supplier's expense. Supplier shall provide prompt, full and good faith cooperation in the performance of the SRA.

13.1.5. Supplier and its Personnel shall fully cooperate with any Gen or Gen appointed third party auditors, including any regulatory investigation of Gen or its affiliates, and shall allow access to any (i) Personnel involved in performance of the services or handling of Gen Data, (ii) premises where the services are being performed; (iii) applications and systems used to perform the services; (iv) data and records kept or created with respect to the services or any agreement in place between Supplier and Gen and/or Supplier and its Personnel.

13.1.6. Gen Restricted Data or Gen Confidential Data shall not be shared with any other third party without prior written agreement from Gen.

13.2. Right to Audit

13.2.1. In addition to Gen's inspection and audit rights as set forth in any relevant Terms (inclduing any data processing agreement), Gen reserves the right to require the Supplier to undertake a Gen Security Risk Assessment at least annually. If Supplier fails to comply with such request within a reasonable timeframe, or if the security questionnaire raises Gen security concerns that are not addressed by Supplier to Gen's satisfaction, Gen reserves the right (in addition to any other audit or other rights it may have) to conduct, or engage a reputable third party auditor to conduct an SRA.

14. INFORMATION SECURITY INCIDENT MANAGEMENT

14.1. Management of information security incidents and improvements

14.1.1. Supplier shall notify Gen immediately, and in no event later than twenty-four (24) hours (unless applicable data protection law or the Terms requires a shorter notice period), if there is a reasonable basis to believe that Gen Restricted Data or Confidential Data may have been compromised, including without limit any unauthorized handling.

14.1.2. Supplier shall inform Gen of the following:

14.1.2.1. A description of the nature of the incident including, where possible, the categories and approximate scale of the incident;

14.1.2.2. The name and contact details of the Supplier contact from whom more information can be obtained; and

14.1.2.3. A description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

14.1.3. Supplier shall work with Gen promptly and in good faith as required to resolve the incident, and in conjunction with any associated investigations.

15. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

15.1. Information security continuity

15.1.1. Supplier agrees to maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) (the "Plans") with respect to the services being performed for Gen.

15.1.2. The Plans must be tested at least annually, a copy may be requested by Gen, and all findings shall be remediated.

15.1.3. At a minimum the Supplier's Plans must include the following requirements:

15.1.3.1. Business Continuity Plan (BCP). The Supplier must maintain a BCP for their essential business functions. A BCP must contain the information necessary to plan for the recovery of each essential business functions. BCPs must document the requirements necessary to execute the recovery strategy. BCPs must include strategies to achieve the essential business function recovery timelines determined in the associated Business Impact Analysis. The BCP must include the following information:

- Executive Summary:
- Plan Overview, including the plan specific recovery objectives
- Scope
- Assumptions
- Business Impact Assessment (BIA)
- Recovery Strategy Details and Recovery Procedures for each of the following effects:
- Loss of Facility
- Loss of Critical Personnel
- Loss of Core Dependencies
- Notification, Escalation and Plan Activation Procedures
- Calls Lists
- Recovery Resource Requirements

15.1.3.2. Disaster Recovery Plan (DRP). Except to the extent superseded by more stringent standards included in the Terms, the following shall apply:

- Supplier shall provide Gen with a DRP relevant to any site, network, system, and/or application used to host Gen websites and data within thirty (30) days of the request.
- DRPs shall include procedures to achieve a Recovery Time Objective (RTO) of four (4) hours or less and Recovery Point Objective (RPO) of no more than one (1) hour.

15.1.3.3. Internet Service Suppliers. Supplier shall maintain at least two Internet Service Suppliers ("ISPs") with multiple paths into the building and traffic shall automatically be rerouted to another carrier.

15.1.3.4. Fire. Supplier's facilities shall contain an automated fire suppression system that will not affect any of the equipment or systems but will immediately extinguish a fire.

15.1.3.5. Bandwidth. Supplier shall maintain two identical routers and an alternate firewall server. The backup router and firewall shall be pre-configured and able to be brought online immediately.

15.1.3.6. Power. Supplier's service facilities shall have multiple sources of power including heavy-duty utility feed, extensive uninterrupted power supply (UPS) battery backup, surge protectors between power feed and UPS, and a back-up generator.

15.1.3.7. Server Failure. Supplier's system shall be redundant to a reasonable degree necessary to meet up time and maintenance requirements.

15.1.4. Upon Supplier's determination of a disaster as defined in the Plan, Supplier shall immediately notify Gen and commence the activities for which it is responsible under the Plan. If Supplier materially breaches its obligations to provide disaster recovery services in accordance with this Section, and, as a result thereof, fails to commence performance of services critical to the operation of Gen's business within the proscribed period, Gen shall have, in addition to any other rights of Gen hereunder, the right to retain a third party to provide such services for so long as the disaster continues, at Supplier's expense. Upon cessation of a disaster, Supplier shall as soon as reasonably practicable, provide Gen with an incident report detailing the reason for the disaster and all actions taken by Supplier to resolve the disaster.

Exhibit C
Software and SAAS Terms

1. **Software terms**. Unless otherwise specified in the applicable Order, the Software license grant will be deemed to be perpetual and Gen and its authorized users may at no additional cost:

a. copy and use Software for non-production purposes (including without limit testing, development, training) and for back-up, archival, disaster recovery, high availability, and temporary migration (including bursting) purposes,

b. allow its third-party contractors, agents and outsourcers to install, use and/or access Software solely on behalf of and for the benefit of Gen, and Gen will be responsible for such third parties' compliance with the Terms,

c. adapt, customize, configure, extend, localize, and/or translate the Software,

d. move or transfer Software licenses from any computer or platform to any other computer or platform(s).

Future Software releases will be backwards compatible and will not result in material degradation of the performance, functionality, or security of such Software. Software documentation will accurately reflect the operation and requirements of the Software. No terms, conditions or disclaimers included in any Software or Software-support documentation (or similar Supplier materials) that are in addition to or inconsistent with the terms of these Terms shall be effective unless expressly agreed to by Gen in a mutually executed amendment to these Terms or applicable Order. Quantity-based user licenses will be deemed to be concurrent users unless expressly stated otherwise in the applicable Order, and any named user Software licenses and entitlements may be transferred from any individual user(s) to any other individual user(s) from time to time.

2. **Software Support.** Unless specified in the applicable Order, technical support and maintenance for all Software ("**Support**") is included at no charge as part of the applicable Software fee. Notwithstanding anything to the contrary, Support includes without limit (and Gen will be entitled to receive):

(a) all Software releases that become generally available for a new platform or language,

(b) all error corrections, workarounds, bug fixes, patches, modifications, enhancements and other updates and upgrades which are released to Supplier's other supported customers. Upon request, Supplier shall provide a listing of all available updates currently available to the Supplier's supported customers. Supplier shall deliver to Gen each update as soon as it is generally available in production release,

(c) all replacement products for any discontinued Software,

(d) a toll-free telephone hotline and/or email account, which shall be staffed on a continuous basis twenty four (24) hours per day and seven (7) days per week throughout the Support period, by individuals skilled in Software technical support matters;

(e) access to a Supplier website that provides diagnostics tools, web-based case submission, answers to frequently asked questions, access to technical support news groups, descriptions of the Supplier's internal support procedures and operations necessary for Gen to fully utilize the Supplier's Support capabilities and other web resources offered to the Supplier's supported customers; and

(f) email notification services for general Support issues.

Should Gen allow the Supplier to directly or remotely access Gen's network(s) during the course of performance of any Support, Supplier may be required to agree to additional terms for secure network access.

3. **Support Procedure and Classification.** Gen shall have the right to contact the Supplier's Support organization in accordance with the procedures specified herein. Initial calls into the Supplier's Support organization will be: (i) serviced by a Support employee within fifteen (15) minutes or placed directly into an expedited Support queue, (ii) logged into the Supplier's call tracking system, and (iii) assigned a case number. Gen shall classify each Support request in accordance with the Severity levels specified below and the Supplier shall take the following actions as specified below. All responses shall at a minimum be provided by the Supplier in English and/or any other language specified by Gen to the extent that skilled Support staffing is available with the requested language capabilities.

- Severity 1 Errors:
  Definition: A problem has been identified that makes the continued use of one or more functions impossible (or severely restricted) on a critical system and prevents continued production or severely risks critical business operations. Problem may cause loss of data and/or restrict data availability and/or cause significant financial impact to Gen.

  Response Commitment: A Support engineer will respond to a call within one (1) hour of a problem report. The Supplier will promptly assign Supplier Support engineers to investigate the problem report and notify the Supplier a Severity 1 Error has been reported and of the steps being taken to correct such error. The Supplier shall provide Gen with at a minimum reports every three (3) hours on the status of the investigation. The Supplier shall initiate work to provide Gen with a workaround or fix. If a workaround or fix is not available within four (4) hours, the problem report shall be escalated to the Supplier's product development organization. The Supplier and its personnel shall provide uninterrupted continuous effort on a 365x24x7 basis until a Severity 1 Error is corrected or a workaround acceptable to Gen is implemented.

- Severity 2 Errors:
  Definition: A problem has been identified that severely affects or restricts major functionality. The problem is of a time sensitive nature and important to long-term productivity but is not causing an immediate work stoppage. No workaround is available and operation can continue in a restricted fashion.

  Response Commitment: A Support engineer will respond to a call within two (2) hours of a problem report. The Supplier will promptly assign Supplier Support engineers to investigate the problem report. Supplier shall initiate work to provide Gen with a workaround or fix. If a workaround or fix is not available within twenty-four (24) hours, the problem report shall be escalated to Supplier Development.

- Severity 3 Errors:
  Definition: A minor problem that does not have major effect on business operations or a major problem for which a Gen acceptable Workaround exists.

  Response Commitment: A Support engineer will respond to a Gen call within two (2) business days of a problem report. Supplier will promptly assign Supplier Support engineers to investigate the problem report. Supplier shall initiate work to provide Gen with a workaround or fix. If a workaround or fix is not available, Supplier may include a fix for the error in a future Releases.

4. **Support Renewal and Cancellation.** For any Software where Support is not included as part of the Software fee:
   a. Gen shall have the right, in its discretion and without obligation, to renew Support in whole or in part and in any quantities,
   b. Support fees (whether for the Software product or for any individual Software licenses) may not increase by more than two percent (2%) per year over those Support fees charged in the immediately preceding year for such Software product or any individual Software licenses,
   c. Supplier shall notify Gen in writing of any Support renewal pricing at least sixty (60) days prior to the expiration of the then-current Support period. If Supplier fails to notify Gen within such period, any purchased Support will be provided at the same rate or net per unit cost as the immediately preceding year.
   d. Gen may renew or reinstate any lapsed Support without any back-charge or additional charge other than the payment of the applicable annual Support fees mutually agreed upon by the parties for the renewal Support period (provided that the Support fee, whether for the Software product or any individual Software license, may not have increased by more than 2% per year since Support for the Software was last made available to Gen),
   e. Gen may cancel Support in part or in whole on not less than 30 days' notice to Supplier, in which case Supplier will refund to Gen any remaining, unused prepaid Support fees for the applicable cancelled Support period, pro-rated on a monthly basis.

5. **SAAS and Hosted Software.** For Software made available as a service or otherwise hosted in whole or in part by or on behalf of Supplier, Supplier makes the following additional terms, representations, and commitments:

   a. Account Management. Supplier will appoint a service level account manager to be the central point of contact for all service levels ("SLA"), general account information and management including Supplier's performance against this SLA,

   b. Software Up-Time:
      (i) "**Minimum Up Time**" means that Software will be available for a minimum of 99.9% Up Time (as defined in the following subsection) each month.
      (ii) "**Up Time**" means (i) the total number of minutes during a calendar month in which the Services are available and usable, excluding time spent on Approved Maintenance, (ii) divided by the total number of minutes during the calendar month. (iii) "**Approved Maintenance**" shall mean notified and scheduled maintenance performed during scheduled maintenance windows.
      (iv) "**Downtime**" means the total number of minutes during calendar month in which the Services are not available and usable, excluding unavailability due to Approved Maintenance or caused by Gen or its third parties (other than compliance with Supplier's instructions).

   c. Failure to maintain the Minimum Up Time. For each month, and for each impacted Software, where there is a failure to maintain Up Time of 99.9%, Supplier shall issue Gen a credit in the following amounts (or pro-rata equivalent if fees are not billed or calculated on a monthly basis):

      - 0 – 1 hour Downtime = no credit
      - 61 minutes - 3 hours Downtime = 5% of all fees billed or due for the applicable month
      - 3 hours and 1 minute - 10 hours Downtime = 25% of all fees billed or due for the applicable month
      - 10 hours and 1 minute - 15 hours Downtime = 50% of all fees billed or due for the applicable month
      - Over 15 hours Downtime = 100% of all fees billed or due for the applicable month

The above Downtime periods are cumulative during the entire month and not limited to a single instance. The credit will be applied to the following month's invoice. For clarity, in the event Services are pre-paid or if no amounts are otherwise owed to Supplier then, in lieu of any credit hereunder, Supplier shall refund the amount of the applicable credit to Gen within thirty (30) days of the end of the month in which the credit accrued. In addition, Supplier shall within ten (10) business days of notice from Gen perform a root cause analysis to identify the cause of such failure, provide a remedy plan and implement such plan in an agreed upon time frame.

d. Maintenance. All scheduled maintenance requiring downtime will be performed between the hours of 12:00 a.m. until 11:59 pm U.S. Central time on Saturdays and Sundays ("**Maintenance Windows**") and require less than 12 hours. Supplier shall provide written notification to Gen at least 7 business days in advance of such maintenance. Any major maintenance or upgrades that will impact the availability of the Services outside the Maintenance Windows must be discussed and expressly approved in writing by Gen in advance.

e. Unscheduled Downtime. In the event of a system failure, Supplier will "fail-over" to an alternate system within 15 minutes and shall bring up the entire infrastructure and the Services from a cold boot in a maximum of one hour. In the event of such a system failure, Supplier will notify Gen of the unscheduled downtime and the status of the event via a telephone conversation. Supplier will escalate the issue within Gen until live human contact is made.

f. Catastrophic Failure. In the event of multiple catastrophic system failures, Supplier shall find a working solution or switch to a backup server in a maximum of twenty-four hours. In the event of such a catastrophic system failure, Supplier will notify Gen of the unscheduled downtime and the status of the event via a telephone conversation. Supplier will escalate the issue within Gen until live human contact is made.

Exhibit D

INTELLECTUAL PROPERTY AGREEMENT

THIS INTELLECTUAL PROPERTY AGREEMENT (the "**IP Agreement**") is entered into by and between Gen Digital Inc. and its affiliates as identified in any Order ("**Gen**") and the seller or provider of any Solutions as identified in such Order ("**Supplier**") if the Supplier is engaged to develop, design, improve, or otherwise work on software, code, or any other technology Solutions for or on behalf of Gen. This IP Agreement shall be effective as of the effective date of the Master Purchase Agreement, Procurement Terms and Conditions, Order or other governing terms between the parties ("**MPA**") by and between Gen and the Supplier which shall occur on the earlier of Supplier's written, electronic, click-through or similar acceptance of the MPA, or on Supplier's provision of any Solutions to Gen which provision shall be deemed to be and relied on as Supplier's affirmative acceptance of the MPA as the governing and superseding document, in satisfaction of all contractual and legal requirements (the "**Effective Date**"). Capitalized terms have the meaning as defined herein or in the MPA. In the event of any conflict or inconsistency between this IP Agreement and the MPA, the terms of the MPA will govern and control.

1. **Intellectual Property**

(a) Developments. Supplier understands and agrees that, to the extent permitted by law, all work, papers, reports, documentation, drawings, images, product or service ideas, computer programs including their source code and object code, rights in databases, prototypes and other materials (collectively, "Developments"), including, without limitation, any and all such Developments generated and maintained on any form of electronic media, that Supplier generates, either alone or jointly with others, under its MPA with Gen will belong to Gen, including any and all copyrights in any and all such Developments. In the event that any portion of the Developments should be deemed not to be owned by Gen, Supplier hereby assigns, conveys, transfers and grants to Gen all of its right, title, and interest in and to the Developments and any copyright therein, and agrees to cooperate with Gen in the execution of appropriate instruments assigning and evidencing such ownership rights. Supplier hereby waives (in favor of Gen and its successors, assigns and licensees) and agrees never to assert against Gen or its licensees any claim or right under moral rights to object to Gen's copyright in or use of the Developments or use of any Pre-Existing Works or Personal Invention licensed to Gen under this IP Agreement.

(b) Inventions. Supplier hereby assigns and agrees to assign to Gen all of its right, title, and interest in and to any device, method, process, discovery or other invention, and any improvements thereon (each an "Invention"), whether patentable or not, that Supplier or its Personnel make, conceive or suggest, either alone or jointly with others, while providing services to Gen ("Assigned Inventions"). Any Assigned Invention and any information pertaining thereto not generally known to the public shall be deemed Confidential Information, as that term is defined in the MPA, and shall be subject to the use and disclosure restrictions therein.

(c) Pre-Existing Works. Supplier owns its Confidential Information and its products, software, materials, tools, technology and know-how, and all intellectual property rights therein, that are independently created or obtained by Supplier other than for Gen (collectively, "Pre-Existing Works"). For any Pre-Existing Works provided to Gen, and for any Developments where ownership does not fully vest with Gen for any reason, Supplier hereby grants Gen a worldwide, royalty free, fully paid, irrevocable right and unrestricted license in and to such Pre-Existing Works and Developments for Gen's business purposes, and without accounting or obligation of any kind to Supplier. "Developments" means all work product and results of services that are created or generated for or on behalf of Gen in the course of providing Solutions to Gen, including without limit all Gen data as input and output by any software Solutions, and any reports or analysis that contain Gen Confidential Information.

(d) Personal Inventions. Inventions that Supplier or its Personnel develop entirely on its or their own time without using Gen's equipment, supplies, facilities, or proprietary information, and that do not relate to Gen's business or result from work performed for Gen under the MPA ("Personal Inventions"), do not belong to Gen. If Supplier believes it or its Personnel have created Personal Inventions during term of the MPA with Gen, Supplier must inform Gen. Supplier hereby agrees not to incorporate, or permit to be incorporated, Personal Inventions in any Assigned Inventions, Developments or Gen product or service in the course of performance of the MPA. Notwithstanding the foregoing, if, in the performance of the MPA with Gen, a Personal Invention is incorporated into any Assigned Invention, Developments, or Gen product or service, then you hereby grant to Gen, under all applicable intellectual property rights, an irrevocable, perpetual, worldwide, transferable, royalty-free, fully paid-up license to make, have made, modify, use, offer to sell, sell, import, export, reproduce, prepare derivative works of, perform, display, distribute and otherwise exploit such Personal Invention, including the right to sublicense these rights to others.

(e) Disclosure of Inventions. Supplier hereby agrees to disclose promptly all Inventions to Gen and to perform, during and after the MPA, all acts deemed necessary or desirable by Gen to permit and assist it, at its expense, in obtaining and enforcing the full benefits, enjoyment, rights and title throughout the world in the Inventions. This includes getting any necessary acts, licenses, assignments or other documentation from Supplier's Personnel or contractors. Such acts may include, without limitation, the execution and delivery of documents and the provision of assistance or cooperation in legal proceedings. In addition, Supplier

hereby irrevocably designates and appoints Gen and its duly authorized officers and agents as its agent and attorney in fact, to act for and in Supplier's behalf and stead to execute and file any such applications and to perform all other lawfully permitted acts to further the securing of Gen's rights in and to the Inventions.

2. **Independent Contractor Status**. Supplier acknowledges and agrees that its relationship, and that of any of Supplier's Personnel, with Gen is that of an independent contractor. This IP Agreement does not constitute a contract of employment with Gen, does not state or imply that Supplier's Personnel are entitled to any employment benefits, and does not obligate Gen to engage Supplier's Personnel for any particular period of time.

3. **Notification**. Supplier hereby authorizes Gen, during and after termination of the MPA with Gen, to notify third parties, including, but not limited to, actual or potential customers or employers, of the terms of this IP Agreement and Supplier's responsibilities hereunder.

4. **Remedies**. This IP Agreement is intended to supplement, and not to diminish, any rights Gen may have in law or equity with respect to the protection of its trade secrets and other intellectual property rights. The meaning, effect, and validity of this IP Agreement will be governed by the laws of the applicable jurisdiction specified in the MPA. You recognize that a threatened or actual breach of this IP Agreement will cause Gen irreparable harm and, therefore, in the event of any violation or threatened violation of this IP Agreement by you, in addition to other remedies Gen may have, Gen will have the right to seek an immediate injunction and the right to recover its reasonable attorney's fees and court costs incurred to enforce this IP Agreement.

5. Survival. Supplier must continue to abide by certain terms of this IP Agreement and MPA even after the termination of the MPA. Those terms are contained in sections 1, 3, 4, 5, and 6 of this IP Agreement, and sections 3 (Confidentiality), 7 (No Publicity; Trademarks), 9 (Software and SAAS License and Additional Terms), 10 (Ownership and License to Pre-Existing Work), 14 (Indemnity), 15 (Limit of Liability), and 21 (Miscellaneous) of the MPA, which shall survive termination of this IP Agreement for any reason whatsoever.

6. **General**. No waiver of any right or remedy relating to this IP Agreement will be binding on Gen unless in writing and signed by an authorized representative of Gen. This IP Agreement may not be modified or changed except in a writing signed by Supplier and an authorized representative of Gen. In the event one or more provisions of this IP Agreement are held to be unenforceable under applicable law, such provisions shall be excluded from this IP Agreement and the remainder of the IP Agreement shall be interpreted as if such provision were so excluded and shall be enforceable in accordance with its terms. This IP Agreement contains all the terms of Supplier's understanding with Gen regarding the subject matter herein and supersedes any previous oral or written communications with Gen regarding the same. Except as otherwise provided in this IP Agreement, this IP Agreement, and the rights and obligations of the parties hereunder, will bind and benefit the parties and their respective successors, assigns, heirs, executors, administrators, and legal representatives. Gen may assign any of its rights and obligations under this IP Agreement. Supplier is not entitled to assign or delegate this IP Agreement or any of its rights or obligations hereunder, whether voluntarily or by operation of law, except with the prior written consent of the Gen.

Supplier has read and understands and accepts the obligations provided herein without reservation. Supplier understands this IP Agreement is entered into as a condition of the MPA with Gen if Supplier is engaged to develop, design, improve, or otherwise work on software, code, or any other technology Solutions or developments for or on behalf of Gen under the MPA.

Exhibit E
Gen Insurance Requirements

1. <u>The following insurance requirements apply to all Suppliers who provide Solutions to Gen entities worldwide, except solely to Gen entities located in Australia and India:</u>

Supplier will maintain the following insurance coverage (or foreign equivalent to the US dollar amounts for Suppliers outside of the US):

(i) Commercial general liability insurance (including contractual liability coverage), or regional equivalent, on an occurrence basis for bodily injury, death, "broad form" property damage, and personal injury, with coverage limits of not less than One Million Dollars ($1,000,000) per occurrence and Two Million dollars ($2,000,000) general aggregate for bodily injury and property damage;
(ii) Auto liability insurance covering all owned, non-owned and hired vehicles, with coverage limits of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and property damage;
(iii) Worker's compensation insurance as required by law in the state where the services will be performed, including employer's liability coverage for injury, disease and death, with coverage limits of not less than One Million Dollars ($1,000,000) per accident and employee;
(iv) Umbrella liability insurance on an occurrence form, for limits of not less than Three Million Dollars ($3,000,000) per occurrence and in the aggregate; and
(v) Professional liability (Errors & Omissions) on an occurrence or claims-made form, for limits of not less than Two Million Dollars ($2,000,000) annual aggregate.
(vi) If Supplier will process Personal Data or PCI, Cyber Liability on an occurrence or claims-made form, for limits of not less than Two Million Dollars ($2,000,000) annual aggregate. If coverage is on a claims made form, the policy will be continued for at least one year after the expiration of this agreement. The applicable Gen entity is to be named as an additional insured and coverage is primary without right of contribution of any insurance carried by Gen insurance policies. To the extent permitted by law, Supplier will have its insurer provides a waiver of subrogation in favor of the applicable Gen legal entity.

Insurance carriers shall be rated A-1 or better by A.M. Best Company. The Gen entity issuing the corresponding purchase order is to be added as an additional insured on the Commercial General Liability policy with a waiver of subrogation in favor of the applicable Gen legal entity. Licensor's Commercial General Liability policy shall be considered primary without right of contribution of any insurance carried by Gen insurance policies. Policies shall contain a Severability of Interests clause. Policies shall provide thirty (30) days written notice prior to cancellation, except in the event of non-payment, which shall require at least ten (10) days' notice.

In no event shall the foregoing coverage limits affect or limit in any manner Supplier's contractual liability for indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under these Terms shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by Gen.

2. <u>The following insurance requirements apply to all Suppliers who provide Solutions to Gen entities solely located in Australia:</u>

Supplier shall obtain and maintain in force with reputable insurers during the term of these Terms such insurance as is required by law in Australia, including Auto Liability and coverage for work place injury, and any coverages which are usual, customary and appropriate for its business according to the Solutions provided. This shall include but is not limited to the following coverage (or foreign equivalent if not in Australian Dollar):

(i) Public and Products Liability – in limits not less than $10,000,000 AUD. The policy shall include an Indemnity to Principal endorsement in favor of Gen.
(ii) Professional Indemnity or IT Liability for damages arising from negligent acts, errors & omissions caused by the Supplier or any subcontractors conducting work on their behalf, with limits of not less than $1,000,000 AUD.
(iii) If Supplier will process Personal Data or PCI, Cyber Liability on an occurrence or claims-made form, for limits of not less than Two Million Dollars ($2,000,000 AUD) annual aggregate. If coverage is on a claims made form, the policy will be continued for at least one year after the expiration of this agreement. The applicable Gen entity is to be named as an additional insured and coverage is primary without right of contribution of any insurance carried by Gen insurance policies.

Supplier's coverage shall be considered primary without right of contribution of Gen's insurance policies. To the extent permitted by law, Supplier will have its insurer provides a waiver of subrogation in favor of the applicable Gen legal entity. In no event shall the

foregoing coverage limits affect or limit in any manner Supplier's contractual liability for Indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under these Terms shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by Gen.

3. <u>The following insurance requirements apply to all Suppliers who provide Solutions solely to Gen entities located in India:</u>

Supplier shall obtain and maintain in force with reputable insurers during the term of these Terms such insurance as is required by law in India, such as Auto Liability, and any coverages which are usual, customary and appropriate for its business according to the Solutions provided. This shall include but is not limited to the following coverages (or foreign equivalent to the US dollar amounts for Suppliers outside of the US):

1) Public Liability insurance in limits not less than the local currency equivalent of $1,000,000 USD, including coverage for Contractual Liability and Personal and Advertising injury.
2) Errors and Omissions insurance for damages arising from negligent acts, errors & omissions caused by the Supplier or any subcontractors conducting work on their behalf, with limits not less than the local currency equivalent of $1,000,000 USD.
3) If Supplier will process Personal Data or PCI, Cyber Liability on an occurrence or claims-made form, for limits of not less than Two Million Dollars ($2,000,000 USD) annual aggregate. If coverage is on a claims made form, the policy will be continued for at least one year after the expiration of this agreement. The applicable Gen entity is to be named as an additional insured and coverage is primary without right of contribution of any insurance carried by Gen insurance policies.

The Gen entity issuing the corresponding purchase order shall be added as an additional insured to Supplier's policies. To the extent permitted by law, Supplier will have its insurers provide a waiver of subrogation in favor of the applicable Gen legal entity.

Supplier's coverage shall be considered primary without right of contribution of Gen's insurance policies. In no event shall the foregoing coverage limits affect or limit in any manner Supplier's contractual liability for Indemnification. Supplier shall be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required of Supplier under this Section. All of Supplier's activities under these Terms shall be at Supplier's own risk, and Supplier's employees and agents shall not be entitled to any benefits under the policies of insurance maintained by Gen.