General Terms and Conditions (the "Terms and Conditions" or the "T&C") of GSK Consumer Healthcare Israel Ltd.

Article 1 - The parties

1. These general conditions are applicable to any agreement between the company mentioned above (hereinafter "**GSK**") and the Supplier.

2. "**Provider**", "**Supplier**" or "**Third Party**" are understood as the individual or legal entity that has delivered or will deliver goods to GSK or provide services of any kind to GSK.

3. "**Contract**" or "**Agreement**" is understood as the written agreement referring to either the delivery of goods to GSK or the rendering of services to GSK as well as the fulfillment of any other obligations agreed between the parties.

4. In the event of incompatibility between these provisions and any delivery terms and conditions used by the Supplier in its activity, these Terms and Conditions will prevail.

Article 2.- Validity

1. The Contracts to which these Terms and Conditions apply are those that have been suitably signed by a GSK representative.

2. Any change to the Contract must be made in writing and signed by a GSK representative.

Article 3.- Delivery of goods

1. In the event that the object of the Contract consists of the delivery of goods to GSK, then at the request of GSK, the Supplier, prior to the shipment of all the goods that have to be delivered to GSK by virtue of the Contract, must send a sample of the goods for its acceptance by GSK.

2. GSK reserves the right to return those deliveries of goods that exceed the quantities requested in the order and/or Contract.

3. Transfer of risks: As long as the delivery of the goods does not take place, the risk for loss or deterioration shall be borne by the Supplier.

4. Quality: GSK will communicate to the Supplier, within thirty (30) days following the delivery of the goods, those that do not meet the qualities, standards and specifications indicated in the Contract. These goods will be returned to the Supplier at the latter's expense. GSK may rescind, in whole or in part, the Contract at their discretion. GSK may require the Supplier to extend the previous term by thirty (30) additional days.

5. Return period: GSK reserves the right to return all goods that are not delivered within the delivery period set in the Contract, as well as to terminate, in whole or in part, the Contract to which they refer, the Supplier recognising and accepting any return that may happen for this reason and the resolution of the same.

Article 4.- Provision of Services

In the event that the object of the Contract consists in the provision of services to GSK by the Supplier, in general GSK will issue the corresponding certificate of conformity. This will imply the fulfilment by the Provider of the agreed levels of service.

If GSK should identify a breach in the agreed level of service indicators, it will inform the Supplier as quickly as possible so that the latter may correct the deviation identified in the level of service.

Article 5.- Price, invoicing and payment method

The prices indicated in the order are firm and for goods placed at the indicated address, unless otherwise agreed in writing.

Unless expressly agreed between GSK and the Supplier in writng, or otherwise indicated by GSK, within ten (10) days following the delivery of the goods or the provision of the corresponding services, the Supplier shall issue the corresponding invoice, which shall include the order number that GSK indicates and shall be sent by the Supplier to GSK by one of the following ways: (i) physically and by ordinary mail to the address designated by GSK and whose information appears on the order issued by GSK or (ii) electronically through e-mail to the mail box stipulated on the order issued by GSK.

The invoice will be paid by GSK within the agreed term by bank transfer to the account indicated by the Supplier for this purpose.

Article 6.- Cancellation

In the event of a breach by the Supplier of any condition established either in the order or the present T&C, GSK, independently of any other rights, may:

1. Rescind the order, or terminate the Contract.

2. require from the Supplier any compensation to which GSK is entitled in accordance with these T&C or applicable law.

Article 7.- Liability and Indemnification.

The Supplier hereby agrees to defend, indemny and holds harmless GSK and its respective officers, directors, agents, contractors, subcontractors, employees, successors and assigns (collectively, the "**Indemnitees**") from and against any and all allegations, losses, demands, claims (including taxes), liabilities, damages (including punitive and exemplary), fines, penalties and interest, and all related costs and expenses of whatever nature (including reasonable attorneys' fees and disbursements and costs of investigation, litigation, experts, settlement, judgment, interest and penalties), and whether by reason of death of or injury to any person or loss of or damage to any property or otherwise from any individual or entity ("**Claims**") arising out of or in any way connected with any of the following: (i) Supplier's breach of the Agreement or this T&C; (ii) the goods and/or services provided by Supplier under the Agreement; and (iii) any related act or failure to act by Supplier, whether or not occurring during the Term or occasioned or contributed to by the negligence of the Indemnitees or agents or employees of the Indemnitees, or any of them (except as and to the extent otherwise prohibited by applicable Law), including Claims related to any act by Supplier that violates or infringes upon, or will violate or infringe upon, in any way the rights of other parties, including non-disclosure rights, privacy rights, Intellectual Property Rights and other proprietary rights.

In the event that any such Claim is made or any action or proceeding is brought against the Indemnitees, or any of them, any such Indemnitee may, by notice to Provider, require Provider, at Provider's expense, to resist such Claim, action or proceeding or take over the defense against such Claim, action or proceeding and employ legal counsel for such purpose (such legal counsel to be subject to the prior approval of such Indemnitee), which approval will be deemed to have been given hereby in the case of legal counsel acting for the insurance underwriters of Provider engaged in such resistance or defense.

If for any reason the foregoing indemnifications are unavailable to the Indemnitee or insufficient to hold any of them harmless, then Provider will reimburse the Indemnitees for all amounts paid or payable by the Indemnitees as a result of such Claims, which will include the costs of defending against any Claims because of Provider's failure to provide the defense specified above. The reimbursement, indemnity and contribution obligations of Provider under this section will be in addition to any liability that Provider may otherwise have, and will extend upon the same terms and conditions to the Indemnitees.

The Supplier assumes full liability for the losses and damages that as a consequence of breach or defective compliance on their part of these T&C may be caused to GSK and/or third parties.

Article 8.- Prevention of corruption

Third Party agrees that it shall comply fully at all times with all applicable laws and regulations, including but not limited to anti-corruption laws, and that it has not, and covenants that it will not, in connection with the performance of this Agreement, directly or indirectly, make, promise, authorise, ratify or offer to make, or take any act in furtherance of any payment or transfer of anything of value for the purpose of influencing, inducing or rewarding any act, omission or decision to secure an improper advantage; or improperly assisting it or GSK in obtaining or retaining business, or in any way with the purpose or effect of public or commercial bribery, and warrants that it has taken reasonable measures to prevent subcontractors, agents or any other third parties, subject to its control or determining influence, from doing so. For the avoidance of doubt, this includes facilitating payments, which are unofficial, improper, small payments or gifts offered or made to government officials to secure or expedite a routine or necessary action to which we are legally entitled.

GSK shall be entitled to terminate this Agreement immediately on written notice to Third Party , if Third Party fails to perform its obligations in accordance with this Clause. Third Party shall have no claim against GSK for compensation for any loss of whatever nature by virtue of the termination of this Agreement in accordance with this Clause.

Third Party shall not contact, or otherwise knowingly meet with any Government Official for the purpose of discussing activities arising out of or in connection with this Agreement, without the prior written approval of GSK and, when requested by GSK, only in the presence of a GSK designated representative.

For the purpose of this agreement "**Government Official"** (where 'government' means all levels and subdivisions of governments, i.e. local, regional, national, administrative, legislative, executive, or judicial, and royal or ruling families) means: (a) any officer or employee of a government or any department, agency or instrumentality of a government (which includes public enterprises, and entities owned or controlled by the state); (b) any officer or employee of a public international organisation such as the World Bank or United Nations; (c) any officer or employee of a political party, or any candidate for public office; (d) any person defined as a government or public official under applicable local laws (including anti-bribery and corruption laws) and not already covered by any of the above; and/or; (e) any person acting in an official capacity for or on behalf of any of the above. "Government Official" shall include any person with close family members who are Government Officials (as defined above) with the capacity, actual or perceived, to influence or take official decisions affecting GSK business.

Third Party shall inform GSK in writing, if, during the course of this Agreement, it is convicted of or pleads guilty to a criminal offence involving fraud or corruption, or becomes the subject of any government investigation for such offenses, or is listed by any government agency as debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for government programs.

Third Party represents and warrants that except as disclosed to GSK in writing prior to the commencement of this Agreement: (1) none of their significant shareholders (>25% shareholding) or senior management have influence over GSK's business; (2) no significant shareholders (>25% shareholding), members of senior management team, members of the Board of Directors, or key individuals who will be responsible for the provision of goods / services, are currently or have been in the past two years a Government Official with actual or perceived influence which could affect GSK business; (3) it is not aware of any immediate relatives (e.g. spouse, parents, children or siblings) of the persons listed in the previous subsection (2) having a public or private role which involves making decisions which could affect GSK business or providing services or products to, or on behalf of GSK; (4) it does not have any other interest which directly or indirectly conflicts with its proper and ethical performance of this Agreement; and (5) it shall maintain arm's length relations with all third parties with which it deals for or on behalf of GSK in performance of this Agreement. Third Party shall inform GSK in writing at the earliest possible opportunity of any conflict of interest as described in this Article 8 that arises during the performance of this Agreement.

GSK shall have the right during the term of the Agreement to conduct an audit of Third Party's activities under the Agreement to monitor compliance with the terms of the Agreement. Third Party shall cooperate fully with such audit, the scope, method, nature and duration of which shall be at the sole reasonable discretion of GSK.

Third Party shall ensure that all transactions under the Agreement are properly and accurately recorded in all material respects on its books and records and each document upon which entries such books and records are based is complete and accurate in all material respects. Third Party must maintain a system of internal accounting controls reasonably designed to ensure that it maintains no off-the-books accounts.

Third Party agrees that in the event that GSK believes that there has been a possible violation of the terms of this Agreement, GSK may make full disclosure of such belief and related information at any time and for any reason to any competent government bodies and its agencies, and to whomsoever GSK determines in good faith has a legitimate need to know.

Third Party shall provide anti-bribery and anti-corruption training to relevant personnel, including any relevant subcontractors, at Third Party who act on behalf of GSK or interact with government officials during the course of any services provided to GSK. Third Party shall provide GSK the opportunity to evaluate the training to determine whether it abides by GSK's standards and shall conduct additional training, as requested by GSK. Third Party, upon request by GSK, shall certify that the anti-bribery and anti-corruption training has taken place.

Article 9. – Labour Rights

Third Party represents and warrants, to the best of its knowledge, that in connection with this Agreement, it respects the human rights of its staff and does not employ child labor, forced labor, unsafe working conditions, or cruel or abusive disciplinary practices in the workplace and that it does not discriminate against any workers on any ground (including race, religion, disability, gender, sexual orientation or gender identity); and that it pays each employee at least the minimum wage, provides each employee with all legally mandated benefits, and complies with the laws on working hours and employment rights in the countries in which it operates. Third Party shall be respectful of its employees right to freedom of association and Third Party shall encourage compliance with these standards by any supplier of goods or services that it uses in performing its obligations under this Agreement.

Unless otherwise required or prohibited by law, Third Party warrants that in relation to its performance of this Agreement:

a) it does not employ engage or otherwise use any child labour in circumstances such that the tasks performed by any such child labour could reasonably be foreseen to cause either physical or emotional impairment to the development of such child

b) it does not use forced labour in any form (prison, indentured, bonded or otherwise) and its employees are not required to lodge original identification papers or monetary deposits on starting work;

c) it provides a safe and healthy workplace, presenting no immediate hazards to its workers. Any housing provided by Third Party to its workers is safe for habitation. Third Party provides access to clean water, food, and emergency healthcare to its workers in the event of accidents or incidents at Third Party 's workplace;

d) it does not discriminate against any workers on any ground (including race, religion, disability, gender, sexual orientation or gender identity);

e) it does not engage in or support the use of corporal punishment, mental, physical, sexual or verbal abuse and does not use cruel or abusive disciplinary practices in the workplace;

f) it pays each employee at least the minimum wage, or a fair representation of the prevailing industry wage, (whichever is the higher) and provides each employee with all legally mandated benefits;

g) it complies with the laws on working hours and employment rights in the countries in which it operates;

h) it is respectful of its employees right to join and form independent trade unions and freedom of association;

Third Party is responsible for controlling its own supply chain and shall encourage compliance with ethical standards and human rights by any subsequent supplier of goods and services that are used by Third Party when performing its obligations under this Agreement.

Third Party shall ensure that it has ethical and human rights policies and an appropriate complaints procedure to deal with any breaches of such policies. In the case of any complaints, Third Party shall report the alleged complaint and proposed remedy to GSK.

GSK reserves the right upon reasonable notice (unless inspection is for cause, in which case no notice shall be necessary) to enter upon Third Party's premises to monitor compliance with the provisions of this Aritcle 9, and Third Party shall, subject to compliance with Applicable Laws, provide to GSK any relevant documents requested by GSK in relation thereto.

Article 10.- Environment, health and safety (EHS)

The Supplier guarantees the following points:

(i) comply with all applicable laws, regulations, licenses, permits, information registrations and restrictions;

(ii) implement, or already has implemented, an Environment, Health and Safety ("**EHS**") policy and risk-based management system with a commitment to provide a safe and healthy workplace and protect the environment;

(iii) ensure there is at least one senior executive with responsibility for EHS and the organisation has access to technical expertise to support the company in meeting EHS legal obligations;

(iv) disclose and report proactively to GSK on incidents requiring notification to EHS regulators and any associated fines, prosecutions or civil actions;

(v) provide relevant information, education and training to workers on the hazards, risks and controls associated with their job;

(vi) provide the physical infrastructure and engineering controls necessary to ensure safe storage, handling and processing of materials and waste in order to protect people, the environment and local communities from harm;

(vii) provide and maintain emergency detection systems and an effective response capability; and

(viii) cooperate fully with the completion of an onsite EHS audit of the manufacturing facility/premises when requested by GSK.

Article 11. – Representations and Warranties.

Supplier hereby represents and warrants that:

(i) Supplier is free to provide GSK with the goods and/or services, upon the terms contained in these T&C's, and there are no contracts and/or restrictive covenants preventing full performance of Supplier's duties and obligations under these T&C's;
(ii) it has the power and authority to execute and deliver the goods and/or services and to perform its obligations hereunder;
(iii) it will perform its duties and obligations with the highest degree of professionalism and to the full satisfaction of GSK.

Article 12.- Intellectual property rights

GSK will hold, exclusively, all intellectual property exploitation rights, and especially those of reproduction, distribution, transformation and public communication, of the contents and materials provided to Supplier in connection with the goods or services and/or prepared by the Supplier within the framework of the Agreement, both in Israel as well as abroad (collectively, "GSK Proprietary Rights"). To the extent permitted under applicable law, all the GSK Proprietary Materials, including any and all intellectual property rights related therein will constitute "works made for hire" by Supplier for the benefit of GSK and its affiliates, and the ownership of such Proprietary Materials will vest in GSK at the time they are created. To the extent that the Proprietary Materials are not "works made for hire" under applicable copyright or other laws, Supplier hereby assigns and transfers to GSK and its affiliates all right, title and interest that Supplier or anyone on its behalf may now or hereafter have in the Proprietary Materials.

Article 13.- Confidentiality

The Supplier undertakes to maintain absolute confidentiality with respect to the information or documentation (henceforth, the "Information") that GSK may provide or disclose in order to allow Supplier to perform the services or deliver the goods covered by these T&C's, as well as not to use of the same for a purpose other than that established within the framework of these T&C's.

Upon termination of the services covered by these T&C's, the Supplier agrees to discontinue all services, cease all use of the Information and, on the written request of GSK, to return to the latter, on time, all the Information, being unable to keep any copy of the same.

The confidentiality commitment contained in this clause shall be maintained for a period of five (5) years from the date of this agreement.

Article 14.- General conditions and jurisdiction

a) **Assignment**. Supplier shall not assign any of its rights and obligations hereunder without the prior written consent of GSK, and any attempt to assign without such consent shall be null and void. GSK may assign the Agreement at its sole discretion.

b) **Governing Law and Jurisdiction**. These T&C's shall be governed by and construed in accordance with Israeli law. The courts in Tel-Aviv, Israel shall have exclusive jurisdiction in relation to any dispute arising out of or in connection with these T&C's.

c) **Exclusivity**. The Agreement is not, and will not be construed as, exclusive and shall not limit GSK from engaging goods and/or services of any other third party, which are equal or similar to the good and/or services rendered hereunder by Supplier.

d) **Waiver**. Either party's failure at any time to require strict compliance by the other party of the provisions of these T&C's shall not diminish such party's right thereafter to demand strict compliance therewith or with any other provision. Waiver of any particular default shall not waive any other default.

e) **Entire Agreement**. These T&C's contain and set forth the entire agreement and understanding between the parties with respect to the subject matter contained herein, and as such supersedes all prior discussions, agreements, representations and understandings in this regard. This Agreement shall not be modified except by an instrument in writing signed by both parties.

f) **Severability**. In the event that any provision of these T&C's shall be deemed unlawful or otherwise unenforceable, such provision shall be severed from these T&C's and all other provisions of these T&C's shall continue in full force and effect.

Particular Terms and Conditions of GlaxoSmithKline (Israel) Ltd. (the "Particular Conditions")

The Particular Conditions will be applicable depending on the nature of the goods or services contracted by GSK from the Supplier.

Article 1 - Crisis & Continuity Management

Third Party must have effective crisis management and business continuity (CCM) plans in place which reflect ISO 22301 standards that are ready for use and that include risk assessment and mitigation, authorised response and recovery strategies for impacts to workforce, facilities, technology, and key suppliers, key areas of responsibility and clear communication routes internally and with GSK before a business disruption occurs. Third Party must update its CCM plan to reflect significant business or organizational changes on every twelve (12) months or less and must test the plan through an exercise or activation every twenty-four (24) months or less.

Third Party must ensure that employees responsible for crisis management and business continuity are trained to implement plans for their areas of responsibility. Third Party must allow GSK to conduct an assessment of the effectiveness of CCM controls and documents upon mutually agreed dates upon no less than 2 weeks' notice. Following that assessment, Third Party shall provide their proposed remedial actions to any matters raised by GSK within 2 weeks of GSK's initial written request. Third Party shall implement any agreed action, including an agreed Time to Recovery for contracted products or services, within 2 months (or otherwise as mutually agreed).

If any business interruption occurs, Third Party shall:

- Communicate this to GSK as soon as reasonably practicable.
- Implement its business continuity plan and/or crisis management plan (as appropriate).
- Continue to undertake the affected Services in accordance with its business continuity plan and/or crisis management plan (as appropriate).
- Restore the affected Services to normal within the period laid out in its business continuity plan and/or crisis management plan (as appropriate).

Article 2 - Inappropriate Promotion

Third Party shall carry out all activities undertaken in connection with any GSK product, or otherwise under this Agreement, in compliance with:

(i) all applicable laws and regulations;
(ii) the requirements of the IFPMA code; and
(iii) applicable local industry codes in the country where the activity is taking place.

Third Party shall carry out all activities undertaken in connection with any GSK product, or otherwise under this Agreement, in compliance with the Standards of Promotion and Scientific Engagement (Prescription Medicines) for Third Parties, together with such material amendments to such Standards as GSK may notify to Third Party from time to time. **Third Party will implement an internal compliance framework to ensure compliance with these requirements.**

As soon as possible, and in any event within 24 hours of becoming aware, Third Party shall disclose to GSK conduct by Third Party or Third Party employees, or by any Third Party sub-contractor, agent or its employees, in connection with GSK products or otherwise in connection with this Agreement that violates or potentially violates any such laws, regulations, codes, guidelines or standards.

Before any employee of Third Party, its agent or its sub-contractor engages in activities in respect of GSK products, or otherwise in connection with this Agreement, Supplier shall ensure that such

personnel are trained on the requirements set out in Clauses above and certify their understanding of, and agreement to follow, these requirements. Third Party shall implement refresher training at own cost of all such personnel annually.

The Parties may agree to implement the Monitoring Plan set out.

Any information and materials in whatever form used by Third Party in connection with the promotion or marketing or sale of GSK products, or otherwise to generate interest in GSK products or the related disease area ("**Materials**") shall require the prior written approval of GSK. In seeking such written approval of GSK, Supplier shall submit specimens of all Materials to GSK.

GSK will disclose all transfers of value (if any) made by Third Party to HCPs/OHS, as required by applicable local laws and industry codes of practice.

Third Party shall comply with the following in connection with the promotion or marketing or sale of GSK products or otherwise the performance of this Agreement:

- Third Party will comply with the monetary limits to any hospitality provided to HCPs/OHS as set out in the appropriated Schedule.

- In the countries listed in the referred Schedule, Third Party may provide cultural courtesy gifts to HCPs/OHS subject to the limits set out in the appropriated Schedule and provided that this is done in a fully transparent way and is informed to GSK prior to implementation.

- Third Party shall obtain GSK's prior written approval for any proposed engagement of an HCP/OHS that involves a transfer of value to the HCP/OHS, in order to enable GSK to apply its overall cap on HCP payments both to GSK payments and to Third Party 's payments. Third Party will provide to GSK such information as GSK may require for GSK to disclose such payments in accordance with applicable laws, regulations or industry codes of practice.

- If, to enable disclosure of transfers of value in accordance with applicable laws or regulations or industry codes of practice, the consent of the HCP/OHS is required to disclosure, Third Party shall not engage an HCP/OHS without receiving in advance the HCP/OHS' written consent to such disclosure that will also consent to GSK disclosure.

- Third Party shall comply with the limits for Sampling as set out and Third Party shall follow the process set out to ensure such compliance.

Notwithstanding any other provisions in this Agreement, Third Party acknowledges that all decisions about compensation of its employees remain the exclusive decision of Third Party subject to its agreement, it will in its performance of this Agreement (including without limitation, its Promotion and Sale of the Products in the Territory) comply with and ensure its agents and contractors comply with certain GSK principles regarding sales force incentives described here:

- Third Party acknowledges that while the ultimate type and form of compensation it provides to its Sales Professionals and First Line Sales Leaders remain its exclusive decision, it shall not and shall ensure that its agents and contractors shall not, provide financial incentives (through compensation, including incentive compensation or otherwise) to its Sales Professionals or their First Line Sales Leaders based on individual sales targets of the Products; and

- Third Party shall allow GSK to review its relevant field sales force compensation plan(s) or other relevant document describing performance expectations applicable to Sales Professionals and First Line Sales Leaders for compliance with this provision.

For the purposes of this Clause, the following words shall have the following meanings:

"Sales Professional" means the Third Party Representative whose role includes direct interaction with prescribing customers involving the Products.

“First Line Sales Leader” means the direct manager of the Sales Professional.

Article 3 - Patient Safety

During the contract duration if the Third Party or any of its sub-contractors becomes aware of Human Safety Information (HSI), including Adverse Events (“AE”) (together referred as HSI/AE) (whether the information relates to the GSK Product by reference to its generic name or by reference to its trade mark) it shall forward such information to GSK.

“GSK Product” is defined as an investigational or licensed medicinal product, consumer healthcare product, vaccine, biological product or device whether under development by, or manufactured, marketed, supplied, or distributed by or on behalf of, any division or operating company of GSK and includes ViiV Healthcare, whether in the Territory or in any other country.

All HSI/AEs shall be reported to GSK within 24 hours of initial receipt (or next working day if over a weekend) using GSK provided HSI/AE form. Reports for this engagement should be sent via secure email/fax to the contact details found on the reporting form.

HSI is defined as information relating to human health and/or wellbeing following exposure to GSK products, including AE information. AE shall mean any untoward medical occurrence in a patient, clinical investigation subject or consumer and is temporally associated with the use of a GSK Product, whether or not related to the product. HSI/AEs can include:

- Any unintended sign (including an abnormal laboratory finding), symptom, or disease (new or exacerbated).
- Failure to produce expected benefits (i.e. lack of efficacy).
- Off-label use.
- Medication errors or misuse, including drug overdose, whether accidental or intentional.
- Drug abuse or effects of drug withdrawal.
- Occupational exposure.
- Patients taking GSK products whilst pregnant or breastfeeding.
- Paternal exposure to a GSK product before and during pregnancy.
- Transmission of an infectious agent via a medicinal product.
- Safety information received as part of a product quality complaint.
- Drug interaction.
- Unexpected therapeutic benefits (i.e. an unexpected improvement in a concurrent condition other than the one being treated).

Third Party confirm that the HSI/AEs that it sends to GSK were sent successfully without error. If a failure notification is received, Third Party shall immediately re-send the HSI/AE and take reasonable steps to ensure it does not occur again. Third Party is responsible to follow all local regulations for reporting of HSI/AEs. The Third Party is required to keep records of successful confirmation and provide upon request by GSK. This information should be readily available in case of audit/inspection.

In no event will personally identifiable information of any patient be provided to GSK in connection with any HSI/AE without consent from the respondent. Personal data of a healthcare professional who has reported an HSI/AE under this Agreement may be disclosed to GSK only where that healthcare professional has given their consent for such disclosure.

CYBER SECURITY SCHEDULE

This Cyber Security Schedule forms a part of the Agreement by and between GSK and Supplier. In the event of any conflict with respect to cyber security between the terms of this Schedule and the terms of the Agreement, this Schedule shall control. Capitalised terms not defined in this Schedule will have the meanings ascribed to them in other parts of the Agreement.

1. Comprehensive Security Program

a. Standards and Documentation. While providing the Services identified in a Service Order or Statement of Work to the Agreement, Supplier will maintain, and will comply at all times with, a comprehensive cyber security program of policies, standard operating procedures ("**SOPs**') and controls governing the Processing, storage, transmission and security of GSK Data (the "**CSP**"). The CSP shall: (a) be consistent with generally-accepted industry standards (e.g., ISO 27001, COBIT, NIST 800-53); (b) require maintenance and annual review and updating of documentation of all requirements, policies, SOPs and other elements of the CSP (collectively, the **"CSP Documentation"**); and (c) be operated by individuals with necessary knowledge, skills, and abilities to competently fulfil responsibilities. Supplier shall test, assess, and evaluate the effectiveness of the CSP as required in this Schedule and shall periodically review and update the CSP to address new and evolving security technologies, changes to industry-standard practices, and changing security threats; provided, however, that no such update will reduce the obligations, commitments, or protections set forth herein.

b. Subcontractors, Vendor Risk Management. Supplier will ensure all Subcontractors with access or who Process GSK Data maintain security standards and processes no less stringent than Supplier standards set forth in its CSP. Supplier shall maintain a continuous vendor risk management program that assesses all Subcontractors that access, store, process or transmit GSK Data for appropriate security controls and cyber security practices, and will only engage Subcontractors who demonstrate compliance with Supplier's CSP or like standards to support the delivery of the Services. For avoidance of doubt, Supplier shall remain liable and responsible for the action, inactions and performance of all obligations performed by any Subcontractor to the same extent as if such actions, inaction or obligations were performed by Supplier.

2. Physical and Administrative Security Measures

a. Physical Security

i. Facilities. Supplier will ensure that GSK Data and areas where GSK Data is Processed are physically secured against unauthorized access.

ii. Media. The CSP shall identify which Supplier Personnel may transfer GSK Data to removable media or portable devices and under what circumstances, and which removable media or portable devices containing GSK Data are permitted to be transported out of a Facility. Supplier shall encrypt all GSK Data stored on any removal media or portable device. Supplier shall remove all GSK Data from any removable or portable media containing GSK Data before such media is disposed of or reused, using a removal method that sanitizes the media and makes recovery of the GSK Data infeasible.

b. Administrative Security

i. Security Awareness and Training. Supplier will ensure written policies, procedures, and standards are published and communicated to Supplier Personnel and relevant external parties as relevant to their job function and responsibilities. Supplier shall provide training at the time of hire and periodically thereafter, not less than annually, to applicable Supplier Personnel on the CSP, and Supplier shall maintain training records that will include when the training was received by Supplier Personnel.

ii. Background Screening. Supplier shall perform background screening on Supplier Personnel at the time of hire that includes, to the extent permitted by Applicable Law in the country of hire, proof of identity using government issued identification documents.

3. Technical Security Measures

a. Data Segregation. Supplier will maintain technical mechanisms to ensure that GSK Data is logically segregated from other Supplier customers' data within the Supplier Environment.

b. Access Management. Supplier will protect access to Supplier Environment by Supplier Personnel by authentication and authorization mechanisms as described below and in the CSP Documentation.

i. Least Privilege. Supplier will grant access privileges based on job requirements and shall ensure access rights are implemented adhering to the "least privilege" approach (i.e., authorized staff will be granted the minimum access required to perform their roles).

ii. Access Credentials. Supplier shall, with respect to Access Credentials it manages and controls: (a) ensure Access Credential secrets are suitably complex; (b) Access Credential secrets are encrypted at rest and in transit; (c) assign unique Access Credentials to Supplier Personnel requiring access to the Supplier Environment; (d) ensure all operational support activities, including modification of security controls, are attributed to a single individual; (e) secure remote access in-line with industry best practice (e.g., multifactor authentication, contextual security, etc.); and (f) promptly revoke or modify access rights of Supplier Personnel when such Supplier Personnel no longer require access due to termination of employment or a change in responsibilities. "**Access Credential**" means the combination of a unique identifiers and secrets assigned or provided to an individual, or inherent in an individual, that provides rights to access Supplier Environment resources.

c. Operations. Supplier shall: (a) use environments for development, testing, and production operation as needed with processes to ensure no unauthorized access or changes are made to the production operational environments; (b) protect GSK Data in all Supplier environments from unauthorized access; (c) not use GSK Data in non-production Supplier systems and platforms such as environments for software evaluation and testing, quality assurance testing, training, development, etc.; and (c) ensure that changes to platform, applications, and production infrastructure of Supplier Environment are evaluated prior to going live in a production environment in order to minimize risk and are implemented following Supplier's then-standard operating procedure for change requests.

d. Logging and Monitoring. Supplier will maintain logs sufficient to definitively attribute access to, and actions performed using, GSK Data in line with industry standards. Supplier will protect logs from unauthorized access, tampering, or destruction. Supplier will regularly monitor logs for security alerts using security information and event management (SIEM) system, or equivalent, and respond to alerts as appropriate in line with industry best practice.

e. Network Security. Supplier will maintain network security protecting the Supplier Environment in line with industry best practices including firewalls, intrusion detection and prevention systems, segregation, access control, and secure routing protocols.

f. Vulnerability Management.

i. Ongoing Security Risk Evaluations. Supplier shall: (a) conduct regular periodic vulnerability scans and at least annual internal and external penetration testing on the Supplier Environment; (b) regularly monitor sources such as software vendor websites and credible cyber security news forums for information regarding pertinent new or emerging cyber security threats and Known Vulnerabilities; (c) remediate any

Significant Vulnerability in accordance with the requirements of Section 5. "**Known Vulnerability**" means those vulnerabilities documented and compiled by reputable unaffiliated third parties, highly regarded within the information technology industry for their cyber security expertise, including the NIST National Vulnerability Database, the Open Web Application Security Project (OWASP), United States Computer Emergency Readiness Team (US-CERT), and UK National Cyber Security Centre (NCSC). "**Significant Vulnerability**" means any non-conformity with any of the security provisions of this cyber Security Schedule, or any technical weakness or operational weakness, that could reasonably be anticipated to result in accidental, unauthorized or unlawful access, destruction, disclosure, disruption, misuse, corruption or modification of GSK Data.

ii. Patching. Supplier will apply applicable security patches promptly following a change management process, with critical or high severity vulnerability security patches implemented within thirty (30) days and other security patches within ninety (90) days.

iii. Malware. Supplier shall maintain control processes in line with industry best practice to detect, prevent, and recovery from malware, viruses and spyware, including updating antivirus, anti-malware and anti-spyware software on regular intervals and centrally logging events for effectiveness of such software products.

g. Hardware and Software. Supplier shall maintain software and hardware used to Process GSK Data at versions supported by the licensor or manufacturer, as applicable.

h. Proprietary Code, Security by Design. Supplier shall maintain a formal written software development lifecycle policy that provides for change control and configuration management. Such policy shall require that Supplier Personnel apply a formal process for software code review, including security standards for the development of such software. Supplier will review all changes to applications and Supplier Environment components, testing as required given the nature of the change, to ensure there is no negative impact on Supplier Environment operations or security.

i. FOSS Compliance and Policy. Supplier will: (a) fully comply with the licenses governing its use of any software within the Supplier Environment or any deliverables, to the extent such software meets the open source definition published at OpenSource.org or the free software definition published by the Free Software Foundation (collectively, "**FOSS**"); (b) update and train its engineering and development teams on Supplier's internal controls for managing its use of any FOSS ("**Supplier's FOSS Policy**"), and (c) fully comply with Supplier's FOSS Policy, including requirements to monitor newsfeeds and other industry resources for Known Vulnerabilities applicable to FOSS and, as appropriate, to upgrade to then-new releases that address Known Vulnerabilities and timely application of verified patches as each becomes available. Supplier's FOSS Policy shall require that Supplier shall use versions of FOSS that are as current as feasible considering available updates. Upon GSK request, Supplier will share its then-current Supplier's FOSS Policy. If GSK or its Affiliates request that Supplier provide information regarding FOSS, Supplier will promptly respond to such requests and will otherwise work with GSK to timely resolve any vulnerabilities or risks reasonably raised by GSK.

j. Mobile Devices. If Supplier permits Supplier Personnel to Process GSK Data on portable computing devices such as a smartphone or tablet computer (collectively, "**Mobile Devices**"), Supplier will maintain a Mobile Device management solution that ensures (i) strong authentication of access to device contents, (ii) strong encryption of data at rest, (iii) remote wipe of devices that are lost or stolen where possible and, (iv) deletion of GSK Data in email or Mobile Device storage. For clarity, Mobile Devices excludes laptop computers.

k. Configuration Management. Supplier shall maintain at all times a current inventory of Supplier Environment systems, including network components, computer systems, applications, network topology diagrams, data centre diagrams and IP addresses.

l. Cryptography. Supplier shall use strong encryption controls to protect all GSK Data from unauthorized disclosure, access or alteration, whether: (a) in transit into or out of the

Supplier Environment over third-party networks, (b) when stored on a Mobile Device or removable media, or (c) on laptop computers.

4. **GSK Audit Rights**.

   a. Audits. GSK or its representatives may inspect, examine and review the systems, records, data, practices and procedures of Supplier (and its Subcontractors) that are used in rendering the Services or any technical, consulting or related professional services under the Agreement to verify the integrity of GSK Data and Supplier's compliance with the confidentiality, data protection and security requirements of the Agreement, including this Schedule; provided that any such GSK audit will be conducted only during business hours and upon reasonable prior notice to Supplier, and not more often than once annually, unless a Security Breach (defined in Section 6) has occurred within the immediately preceding ninety (90) days or in the case of an audit conducted by a regulatory authority, in which case notice may be reduced. GSK will comply with Supplier's reasonable security requirements while conducting any audit. GSK shall bear its own expenses, and Supplier and its Subcontractors will reasonably cooperate with GSK and its designated auditors, in connection with any audit.

   b. Annual Third-Party Audit. If Supplier engages an independent third-party auditor to audit its compliance with the Standard and deliver to Supplier a SSAE18 SOC 2 Type II or ISAE3402 or equivalent attestation standard audit report (the "**Annual Audit Report**"), Supplier shall provide a copy of its then-most-recent Annual Audit Report within one (1) week of GSK's request.

   c. Supplier Self-Assessment. Supplier shall conduct not less than annually a self-assessment of its compliance with all requirements set forth in this Schedule.

5. **Remediation**. With respect to any (a) Significant Vulnerability in the Supplier Environment, or (b) non-compliance with this Schedule or Applicable Law revealed to or identified by Supplier, Supplier shall correct or remediate such Significant Vulnerability promptly, or as soon as reasonably possible, in each instance by following the applicable procedures and standards set forth in Supplier's then-current CSP.

6. **Security Breach**. Supplier will report to GSK by email to cstd@gsk.com any verified accidental, unauthorized or unlawful use, loss, destruction, disclosure, access, corruption, modification, sale, rental or other Processing of any GSK Data (a "**Security Breach**") within twenty-four (24) hours of Supplier's verification. Supplier will activate and follow the requirements of Supplier's incident response plan, including requirements and processes for post-mortem reviews, root cause analysis and remediation plans and timelines. As information about the root cause and implications of the Security Breach become known, Supplier shall provide to GSK any further information regarding the nature and consequences of the Security Breach, including any information shared with other customers of Supplier.

ANNEX 1 – DEFINITIONS

"Confidential Information" means all information provided by or on behalf of either Party (the "**Disclosing Party**") to the other Party, its Affiliates, agents, employees or Subcontractors (collectively, the "**Receiving Party**"), (or, in the case of GSK, confidential information of GSK and/or its Affiliates which is obtained by Supplier or Supplier Personnel in connection with exercise of GSK's or its Affiliates' rights or the performance of Supplier's obligations hereunder), which is (a) marked or otherwise identified as "confidential" or with a similar designation, or (b) information that a reasonable person would recognise is information that is confidential given the nature of the information and the circumstances of its disclosure. Confidential Information includes a Party's or its Affiliates' trade secrets, know-how, formulae and processes, scientific research, clinical development, or business affairs; project and technology-related matters, including design/performance specifications, operating procedures, systems documentation, utility reference manuals, language reference manuals, software and documentation, financial information, inventions, contractual information (including pending deals), customer information (including patient and supplier lists), prices and costs, and data related to regulatory submissions. For avoidance of doubt, "**GSK Confidential Information**" means the Confidential Information of GSK and its Affiliates and includes GSK Data and Personal Information.

"GSK Data" means all text, files, images, graphics, illustrations, information, data (including Personal Information or Personal Data, as that term is described in the Data Privacy Schedule), audio, video, photographs and any other content and materials, in any format, that is provided by or on behalf of GSK or obtained by Supplier or Supplier Personnel in connection with or the performance of Supplier's obligations under this Agreement, including any derivatives of such data or information. GSK Data includes any such data or information that either (a) is created, generated, collected or Processed by Supplier Personnel in the performance of Supplier's obligations under the Agreement, or (b) resides in, or runs on or through, the Supplier Environment, or is accessed through GSK's information systems, as well as any output, copies, reproductions, improvements, modifications, adaptations, translations or other derivative works of, based on, derived from or otherwise using such data and information. For the avoidance of doubt, GSK Data: (i) includes all GSK Confidential Information, and (ii) excludes Supplier Confidential Information.

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

"Subcontractor" means any third party (including Supplier Affiliates) who performs on behalf of Supplier or any Subcontractor: (a) any part of the Services or (b) any of Supplier's or a Subcontractor's obligations under this Agreement or any Service Order or Statement of Work.

"**Services**" means the professional, maintenance, consulting, implementation, technical, training or other services identified in the Agreement.

"Supplier Environment" means the combination of hardware, software, operating systems, database systems, tools and network components used by or on behalf of Supplier to receive, maintain, Process, store, access or transmit GSK Data.

"Supplier Personnel" means any and all personnel engaged or employed by Supplier and its Subcontractors to perform any part of the Services.

DATA PRIVACY SCHEDULE

A. **Personal Information.**

i) Each party acknowledges that, for the purpose of laws applicable to any information that can or may be used whether alone or in combination with other information in order to identify a single person ("Personal Information"), GSK is the database owner (also known as the controller) of the GSK Personal Information and Supplier is the database holder (also known as the processor).

ii) Before processing any GSK Personal Information Supplier shall ensure, taking into account industry good practice, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, that appropriate technical and organisational controls are in place to prevent unauthorised or unlawful processing of any such Personal Information it may hold and to protect any such Personal Information from accidental loss, damage or destruction.

iii) Supplier shall:

a) only process GSK Personal Information in accordance with the documented instructions of GSK (including to the extent necessary to comply with its obligations under the Agreement);

b) inform GSK if, in Supplier's opinion, any of GSK's instructions would breach applicable data protection and privacy laws;

c) maintain and implement sufficient and appropriate environmental, physical and logical measures in order to prevent penetration and unauthorized access to GSK Personal Information; and

d) assist GSK with undertaking an assessment of the impact of processing GSK Personal Informationif and to the extent an assessment is required to be carried out under applicable data protection and privacy laws.

B. **Data Subject Rights**

Supplier shall:

i) implement appropriate technical and organisational measures for the fulfilment of GSK's obligation to respond to requests by data subjects to exercise their rights of access, rectification or erasure; and

ii) if a data subject makes a written request to Supplier to exercise any of the rights referred to in clause 15(B)(i), forward the request to GSK promptly, and in any event within five (5) days from the date on which Supplier received the request, and upon GSK's reasonable written request, provide GSK with all co-operation and assistance reasonably requested by GSK in relation to that request to enable GSK to respond to that request in compliance with applicable deadlines and information requirements.

C. **Sharing of Personal Information**

Supplier shall:

i) not engage another processor without prior specific or general written authorisation of GSK and, in the case of general written authorisation, inform GSK of any intended changes concerning the addition or replacement of other processors, thereby giving GSK the opportunity to object to such changes;

ii) before disclosing GSK Personal Information to any processor, enter into a contract with that processor under which the processor agrees to comply with obligations equivalent to those set out in the Agreement, including this Schedule;

iii) notwithstanding the foregoing, Supplier shall remain fully liable to GSK for the performance of any sub-processor's obligations; and

iv) before disclosing GSK Personal Information to any of its employees and representatives, and the employees and representatives of each of its processors, in each case who have access to the GSK Personal Information, ensure that those persons:

a) have undergone appropriate training in data protection and the care and handling of Personal Information; and

b) are bound to hold the information in confidence to at least the same standard as required under this Agreement (whether under a written agreement or otherwise).

v) Upon request, Supplier will provide GSK an annual written report in sufficient detail, pertaining to its compliance to the applicable data protection and privacy Laws in the performance of the services and/or delivery of goods.

D. **No Transfer.**

The Supplier shall not transfer any GSK Personal Information to any jurisdiction not previously agreed in writing with GSK, or transfer any GSK Personal Information to any third party, without the further prior written consent of GSK, which consent may be subject to the Supplier (or the relevant third party) entering into a data transfer agreement with GSK and entering into such other arrangements as GSK may reasonably require to satisfy the requirements that GSK or any of its affiliates may have as data controllers under any applicable law. Where GSK consents to any such transfer, Supplier shall comply with the applicable law governing the transfer of Personal Information to a jurisdiction different from that in which the data Processing is currently performed.

E. **Third Party Data.**

All or part of the GSK Personal Information may contain data that is licensed to GSK by third parties. At GSK's request, Supplier shall enter into any agreements with such third parties as may reasonably be required to enable the processing of the GSK Personal Information.

F. **Compliance with Data protection Laws.**

i. Supplier will promptly notify GSK if it receives any complaint, notice or communication which relates directly or indirectly to the Processing of the Personal Information, or to either party's compliance with data protection laws, and shall fully co-operate and assist GSK in relation to any such complaint, notice, communication or non-compliance; and

ii. Supplier will, upon GSK's reasonable written request, provide all information necessary to demonstrate compliance with these terms, and allow GSK or an auditor appointed by GSK to carry out audits, including inspections of facilities, equipment, documents and electronic data, relating to the Processing of GSK Personal Information by Supplier or any processor, to verify compliance with these terms.

G. **Data Breach**

i. Immediately upon becoming aware of any event raising concern regarding a breach of the GSK Personal Information integrity, unauthorized use thereof or deviation from authorization ("**Data Breach**"), and in any event, not later than 24 hours after becoming aware of that breach, Supplier shall (i) notify GSK of the breach; and (ii) provide GSK all information necessary for GSK to meet its obligations under applicable data protection and privacy laws, including any reporting obligations.

ii. Without derogating from the generality of the above, the information to be provided to GSK by Supplier shall include, without limitation, (i) a description of the nature of the Data Breach; (ii) the categories and numbers of data subjects concerned, and the categories and numbers of GSK Personal Information records concerned; (iii) a description of the likely consequences of the Data Breach; and (iv) a description of the measures taken or proposed to be taken to address the Data Breach, including measures to mitigate its possible adverse effects.

iii. Supplier shall cooperate with GSK in all reasonable and lawful efforts to prevent, mitigate or rectify such data breach and promptly take all necessary steps and corrective actions required by GSK to investigate and handle any data breach affecting GSK Personal Information. Supplier shall document any Data Breach affecting GSK Personal Information (including the facts relating to the breach, its effects and the remedial actions taken) in a sufficient manner to enable GSK to demonstrate compliance with any applicable data protection and privacy Law.

iv. It is hereby agreed that to the extent any reporting obligation applies with respect to the Data Breach, such shall be made by GSK and Supplier shall not make any notification, publication or any other communication relating to the Data Breach, without obtaining GSK's prior written consent.