

General Terms and Conditions (the “Terms and Conditions” or the “T&C”) of ViiVHiV Healthcare Unipessoal, Lda.

Article 1.- The parties

1. These general conditions are applicable to any agreement between the company mentioned above (hereinafter "VIIV") 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 VIIV or provide services of any kind to VIIV.
3. "Contract" or "Agreement" is understood as the written agreement referring to either the delivery of goods to VIIV or the rendering of services to VIIV as well as the fulfilment 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 conditions apply are those that have been suitably signed by a VIIV representative.
2. Any change to the Contract must be made in writing and signed by a VIIV representative.

Article 3.- Delivery of goods

1. In the event that the object of the contract consists of the delivery of goods to VIIV, at the request of VIIV, the supplier, prior to the shipment of all the goods that have to be delivered to VIIV by virtue of the Contract, must send a sample of the product for its acceptance by VIIV.
2. VIIV 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: VIIV 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. VIIV may rescind the Contract at their discretion. VIIV may require the Supplier to extend the previous term by thirty (30) additional days.
5. Return period: VIIV reserves the right to return all merchandise that is 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 VIIV by the Supplier, in general VIIV will issue the corresponding certificate of conformity. This will imply the fulfilment by the Provider of the agreed levels of service.

If VIIV 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.

Unless expressly agreed between VIIV and the Supplier, or otherwise indicated by VIIV, within ten (10) days following the delivery of the merchandise or the provision of the corresponding services, the Supplier shall issue the corresponding invoice, which shall include the order number that VIIV indicates and shall be sent by the Supplier to VIIV by one of the following ways (i) physically and by ordinary mail to the company Recall designated by VIIV and whose data appears on the order issued by VIIV or (ii) electronically through the portal of the electronic invoicing company -Tungsten- designated by VIIV.

The invoice will be paid by VIIV 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, VIIV, independently of any other rights, may:

1. Rescind the order or terminate the Contract.
2. require from the Supplier any compensation to which VIIV is entitled in accordance with these T&C or applicable regulations.

Article 7.- Liability

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 VIIV 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 VIIV 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.

VIIV 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 VIIV 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 VIIV and, when requested by VIIV, only in the presence of a VIIV 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 VIIV business.

Third Party shall inform VIIV 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 VIIV in writing prior to the commencement of this Agreement: (1) none of their significant shareholders (>25% shareholding) or senior management have influence over VIIV'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 VIIV 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 VIIV business or providing services or products to, or on behalf of VIIV; (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 VIIV in performance of this Agreement. Third Party shall inform VIIV in writing at the earliest possible opportunity of any conflict of interest as described in this Article that arises during the performance of this Agreement.

VIIV shall have the right during the terms of this Agreement to conduct an audit of Third Party's activities under this Agreement to monitor compliance with the terms of this 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 VIIV.

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 VIIV believes that there has been a possible violation of the terms of this Agreement, VIIV 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 VIIV 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 VIIV or interact with government officials during the course of any services provided to VIIV. Third Party shall provide VIIV the opportunity to evaluate the training to determine whether it abides by VIIV's standards and shall conduct additional training, as requested by VIIV. Third Party, upon request by VIIV, shall certify that the anti-bribery and anti-corruption training has taken place.

Article 9.- Labour Rights

Unless otherwise required or prohibited by law, Third Party represents and warrants, to the best of its knowledge, that in relation to its performance of this Agreement, it respects the human rights of its staff and:

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 VIIV.

VIIV 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 Article, and Third Party shall, subject to compliance with Applicable Laws, provide to VIIV any relevant documents requested by VIIV 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 VIIV 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 VIIV.

Article 11.- Intellectual property rights

VIIV will hold, exclusively, all intellectual property exploitation rights, and especially those of reproduction, distribution, transformation and public communication, of the contents and materials prepared by the Supplier within the framework of this Agreement, both in Portugal as well as abroad during the maximum duration of the exploitation rights of the works established in articles 26 and 28 of the Consolidated text of the Intellectual Property Law.

Article 12.- Confidentiality

The Supplier undertakes to maintain absolute confidentiality with respect to the information or documentation (henceforth, the "Information") that VIIV may provide in order to perform the services covered by this Agreement, as well as not to use of the same for a purpose other than that established within the framework of this Agreement.

Upon termination of the services covered by this Agreement, the Supplier agrees to cease all use of the Information and, on the written request of VIIV, 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 13.- General conditions and jurisdiction

In everything not foreseen in the present T&C, VIIV and the Supplier refer to the Portuguese regulations, and in particular to the Common Civil Law.

For the solution of any discrepancy with respect to the present T&C, VIIV and the Supplier submit to the jurisdiction of the courts and tribunals of the city of Lisbon, expressly renouncing the jurisdiction that may correspond to them.

Particular Terms and Conditions of ViiVHiv Healthcare Unipessoal, Lda. (the “Particular Conditions”)

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

Article 1.- Animal Welfare

1.a. - For services that implicate the involvement of animals and for services related to studies or analyses that implicate the supply of compounds or the use of animals:

1.a.1. Third Party agrees to comply with all relevant statutes, legislation, regulations and guidelines for the care, welfare and ethical treatment of animals in the country where the Study or Services are being performed. Third Party further agrees to comply with the “3Rs” Principles – reducing the number of animals used, replacing animal with non-animal methods whenever possible and refining the research techniques used. All work must be conducted in adherence to the core principles for animals identified below. Local customs, norms, practices or laws may be additive to the core principles, but Third Party agrees to comply and shall procure and ensure that those acting for or on behalf of Third Party (including its subcontractors) comply, as a minimum, with these core principles:

- a. access to species appropriate food and water;
- b. access to species specific housing, including species appropriate temperature and humidity levels;
- c. provision of humane care and a program of veterinary care through guidance of a veterinarian;
- d. animal housing that minimizes the development of abnormal behaviors;
- e. adherence to principles of replacement, refinement and reduction in the design of in vivo or ex vivo studies with processes to optimize animal use and to ensure effective population management;
- f. supported by a relevant scientific justification/rationale, approved by an institutional ethical review process and subjected to independent scientific review;
- g. commitment to minimizing pain and distress during in vivo and ex vivo studies;
- h. work is performed by staff documented as trained and competent to conduct the procedures for which they are responsible.

1.a.2. Third Party agrees that all Study protocols shall undergo an ethical review, whether or not required by applicable law, and that written documentation confirming ethical review shall be maintained by Third Party until three (3) years after the termination of this Agreement demonstrating that the review was completed. Those records shall be eligible for inspection by ViiV upon reasonable notice and shall be promptly provided to ViiV upon request, provided that such inspection shall not extend to those parts of the records which Third Party can demonstrate to be subject to confidentiality arrangements with other customers. Third Party shall ensure that those acting for or on its behalf (including but not limited to subcontractors) will comply with the obligations identified in this subsection 2.

1.a.3. If Third Party is currently accredited by AAALACi the Contractor agrees to make commercially reasonable efforts to maintain its AAALACi accreditation during the life of this Agreement.

1.a.4. Third Party shall conduct Services and VIIV Studies only through appropriately trained and qualified staff, and Third Party agrees to have policies or procedures in place to ensure the qualification and training of its employees. Third Party shall ensure that those acting for or on its behalf (including but not limited to subcontractors) will comply with the obligations identified in this subsection 4.

1.a.5. Upon reasonable advance notice, VIIV (or its subcontractor/delegate) shall have the right to inspect Third Party's records and facilities. The scope of the inspection may include, but need not be limited to, a tour of the facility, the opportunity to view relevant SOPs, training records, building management records, animal health records, ethical review documents, and any other documents reasonably necessary to assess compliance by Third Party with any of the terms of this Agreement provided that such inspection shall not extend to those parts of the records and facilities which Third Party can demonstrate to be subject to confidentiality arrangements with other customers. To the extent that any significant deficiencies are identified as the result of such inspection, Third Party shall endeavor in good faith to take reasonable and practical corrective measures to remedy any such material deficiencies.

1.a.6. Third Party shall promptly provide to VIIV information of any significant deficiencies identified having regard to its animal care and welfare programme and any corrective actions taken. Third Party shall also provide VIIV copies of any regulatory enforcement action or inspection findings issued to Third Party (or subcontractor) and relating to systemic failure in the ethical care and treatment of animals, regardless of whether such enforcement action or inspection finding relates to a Study associated with this Agreement. Third Party shall ensure that those acting for or on its behalf (including but not limited to subcontractors) will comply with the obligations identified in this subsection 6.

1.a.7. Third Party shall have a procedure in place to assess and approve its external suppliers and distributors who supply animals to Third Party to (i) ascertain and confirm the quality of the animals supplied, (ii) ensure legal requirements for the care and welfare of animals are met and (iii) ensure that only purposebred animals are used to conduct Studies and provide Services. The distance of suppliers from Third Party's test facility shall be minimized (where practicable) and transport processes (e.g. stocking densities, carrying crates, food and water) must ensure minimum stress. On arrival, Third Party shall ensure checks are in place to confirm only healthy animals are used in the Studies. Third Party shall document the approval of its animal suppliers and distributors, which documentation shall be made available to VIIV upon request. VIIV shall have the right, but not the obligation, to approve any supplier of non-human primates or other animals, which right may be invoked upon notice to Third Party.

1.a.8. (Only applicable in the case of services that implicate the involvement of animals). Third Party shall make and retain complete and systematic written records of Third Party's business operations in connection with the performance of this Agreement, and Third Party shall retain all such records for a period as required by applicable law or for three (3) years after work is completed under this Agreement, whichever is greater. The obligations of this Section shall survive termination of this Agreement.

1.b. - For services with substance transfer that implicate the supply of compounds or the use of animals.

1.b.1. Third Party agrees to comply with all relevant statutes, legislation, regulations and guidelines for the care, welfare and ethical treatment of animals in the country where the Study or Services are being performed. Third Party further agrees to comply with the "3Rs" Principles – reducing the number of animals used, replacing animal with non-animal methods whenever possible and refining the research techniques used. All work must be conducted in adherence to the core principles for animals identified below. Local customs, norms, practices or laws may be additive to the core principles, but Third Party agrees to comply and shall procure and ensure that those acting for or on behalf of Third Party (including its subcontractors) comply, as a minimum, with these core principles:

- a. access to species appropriate food and water;

- b. access to species specific housing, including species appropriate temperature and humidity levels;
- c. provision of humane care and a program of veterinary care through guidance of a veterinarian;
- d. animal housing that minimizes the development of abnormal behaviours;
- e. adherence to principles of replacement, refinement and reduction in the design of in vivo or ex vivo studies with processes to optimize animal use and to ensure effective population management;
- f. supported by a relevant scientific justification/rationale, approved by an institutional ethical review process and subjected to independent scientific review;
- g. commitment to minimizing pain and distress during in vivo and ex vivo studies;
- h. work is performed by staff documented as trained and competent to conduct the procedures for which they are responsible.

1.b.2. Upon reasonable advance notice, VIIV (or its subcontractor/delegate) shall have the right to inspect Third Party's records and facilities. The scope of the inspection may include, but need not be limited to, a tour of the facility, the opportunity to view relevant SOPs, training records, building management records, animal health records, ethical review documents, and any other documents reasonably necessary to assess compliance by Third Party with any of the terms of this Agreement provided that such inspection shall not extend to those parts of the records and facilities which Third Party can demonstrate to be subject to confidentiality arrangements with other customers. To the extent that any significant deficiencies are identified as the result of such inspection, Third Party shall endeavour in good faith to take reasonable and practical corrective measures to remedy any such material deficiencies.

Article 2.- Conflict Minerals

The Third Party warrants that in relation to its performance of this Agreement it does not extract, trade, handle or export mineral ores containing: (i) tin (cassiterite); (ii) tantalum (columbite-tantalite or coltan); (iii) tungsten (wolframite); or (iv) gold (together, "**Conflict Minerals**"), which may have originated directly or indirectly from the Democratic Republic of Congo and neighbouring countries, or otherwise operates a robust auditing process to ensure that any such Conflict Minerals do not originate directly or indirectly from Democratic Republic of Congo and neighbouring countries.

Article 3.- 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 VIIV before a business disruption occurs. Third Party must update its CCM plan to reflect significant business or organizational changes or 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 VIIV 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 VIIV within 2 weeks of VIIV'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 VIIV 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 4.- Inappropriate Promotion

Third Party shall carry out all activities undertaken in connection with any VIIV 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 VIIV 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 VIIV 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 VIIV conduct by Third Party or Third Party employees, or by any Third Party sub-contractor, agent or its employees, in connection with VIIV 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 VIIV 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 VIIV products, or otherwise to generate interest in VIIV products or the related disease area ("**Materials**") shall require the prior written approval of VIIV. In seeking such written approval of VIIV, Supplier shall submit specimens of all Materials to VIIV

VIIV 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 VIIV 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 VIIV prior to implementation.

- Third Party shall obtain VIIV'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 VIIV to apply its overall cap on HCP payments both to VIIV payments and to Third Party's payments. Third Party will provide to VIIV such information as VIIV may require for VIIV 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 VIIV 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 VIIV 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 VIIV 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 5.- 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 VIIV.

"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 VIIV within 24 hours of initial receipt (or next working day if over a weekend) using VIIV 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 VIIV 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 VIIV 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 VIIV. This information should be readily available in case of audit/inspection.

In no event will personally identifiable information of any patient be provided to VIIV 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 VIIV 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 VIIV 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 VIIV 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 VIIV 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 VIIV 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 VIIV Data and areas where VIIV Data is Processed are physically secured against unauthorized access.
 - ii. Media. The CSP shall identify which Supplier Personnel may transfer VIIV Data to removable media or portable devices and under what circumstances, and which removable media or portable devices containing VIIV Data are permitted to be transported out of a Facility. Supplier shall encrypt all VIIV Data stored on any removal media or portable device. Supplier shall remove all VIIV Data from any removable or portable media containing VIIV Data before such media is disposed of or reused, using a removal method that sanitizes the media and makes recovery of the VIIV 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 VIIV 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 VIIV Data in all Supplier environments from unauthorized access; (c) not use VIIV 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, VIIV 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 VIIV 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 VIIV 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 VIIV request, Supplier will share its then-current Supplier’s FOSS Policy. If VIIV or its Affiliates request that Supplier provide information regarding FOSS, Supplier will promptly respond to such requests and will otherwise work with VIIV to timely resolve any vulnerabilities or risks reasonably raised by VIIV.
- j. **Mobile Devices.** If Supplier permits Supplier Personnel to Process VIIV 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 VIIV 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 VIIV 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. VIIV Audit Rights.

- a. Audits. VIIV 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 VIIV Data and Supplier's compliance with the confidentiality, data protection and security requirements of the Agreement, including this Schedule [X]; provided that any such VIIV 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. VIIV will comply with Supplier's reasonable security requirements while conducting any audit. VIIV shall bear its own expenses, and Supplier and its Subcontractors will reasonably cooperate with VIIV 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 VIIV'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 VIIV by email to cstd@ViiV.com any verified accidental, unauthorized or unlawful use, loss, destruction, disclosure, access, corruption, modification, sale, rental or other Processing of any VIIV 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 VIIV 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 VIIV, confidential information of VIIV and/or its Affiliates which is obtained by Supplier or Supplier Personnel in connection with exercise of VIIV’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, **“VIIV Confidential Information”** means the Confidential Information of VIIV and its Affiliates and includes VIIV Data and Personal Information.

“VIIV 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 VIIV 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. VIIV 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 VIIV’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, VIIV Data: (i) includes all VIIV Confidential Information, and (ii) excludes Supplier Confidential Information.

“Personal Information” means any information relating to an identified or identifiable individual.

“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 VIIV 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

PROCESSOR TERMS – BASIC PERSONAL INFORMATION

Data Protection Laws means: (a) the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and any applicable laws and/or regulations that implement and/or exercise derogations under it and/or replace or supersede it (including as it forms part of retained EU law as defined in the European Union (Withdrawal) Act 2018) (**GDPR**); and (b) the Data Protection Act 2018; (c) the California Consumer Privacy Act of 2018 (Cal. Civ. Code 1798.100 – 1798.199) (CCPA); and (d) all other laws concerning the processing of personal data;

VIIV Personal Information means any personal data used for the purpose of the Services that is: (i) supplied by or on behalf of VIIV to Supplier (including where Supplier has access to personal data held by VIIV or on its behalf), or which Supplier collects or generates on behalf of VIIV; (ii) that is processed by Supplier under or in connection with this Agreement including: first name and/or last name, initials, work contact details, group memberships, network or user identification number, work history and skills, gender or title, event attendance of VIIV employees and complementary workers using the Services; and (iii) in respect of which VIIV is a controller or owner (or equivalent); and

Security Schedule means the Cyber Security Schedule.

The terms **controller, data protection impact assessment, data subject, personal data, personal data breach, processor, processing, service provider** and **supervisory authority** shall be as defined under relevant Data Protection Laws.

- 1) Each party shall comply with its obligations under applicable Data Protection Laws. VIIV and Supplier acknowledge that the status of each party is a question of fact determined under Data Protection Laws. Without limiting the foregoing, VIIV and Supplier agree that in relation to the VIIV Personal Information processed under this Agreement, for purposes of the CCPA, Supplier is a service provider to VIIV and the processing of VIIV Personal Information by Supplier shall be undertaken for only for VIIV's purposes in accordance with this Schedule, that that no monetary or other valuable consideration is being provided by Supplier to VIIV and therefore VIIV is not selling VIIV Personal Information to Supplier as defined by the CCPA.
- 2) Supplier shall comply with the following in respect of VIIV Personal Information:
 - a) process VIIV Personal Information only on VIIV's lawful written instructions and solely for the purposes of the provision of services by Supplier to VIIV under this Agreement;
 - b) neither Supplier, nor any of its nor any of its employees, agents, consultants or assigns shall have any right to process VIIV Personal Information for their own commercial benefit in any form;
 - c) implement and maintain appropriate technical and organisational security measures, including without limitation, the measures set out in the Security Schedule. References in the Security Schedule to "VIIV Data" shall include VIIV Personal Information;
 - d) keep VIIV Personal Information confidential in accordance with the terms of this Agreement and references in this Agreement and the Security Schedule to VIIV Confidential Information shall include VIIV Personal Information;
 - e) impose confidentiality obligations equivalent to the obligations set out in Article 12 on relevant personnel having access to VIIV Personal Information;
 - f) not engage another processor (a sub-processor) without the prior written approval of VIIV (and for these purposes VIIV consents to the following categories of sub-processor [hosting infrastructure service providers, the use of individual contractors]); and transfer VIIV Personal Information to such approved sub-processors only under a written contract which imposes obligations consistent with those set out in this Schedule;
 - g) provide VIIV reasonable assistance with (i) carrying out any legally required data protection impact assessments; (ii) complying with the rights of data subjects; and (iii)

- responding to requests from any supervisory authority in respect of VIIV Personal Information;
- h) notify VIIV without delay after becoming aware of a personal data breach in respect of any VIIV Personal Information and provide VIIV assistance in relation to such breach;
 - i) notify VIIV without delay if it receives a written request from (i) a data subject to exercise any of their rights in relation to VIIV Personal Information under Data Protection Laws; or (ii) a supervisory authority in relation to the processing of VIIV Personal Information;
 - j) unless otherwise set out in this Agreement, either return or destroy all VIIV Personal Information in its possession or under its control (including any VIIV Personal Information processed by permitted sub-processors) on termination or expiry of this Agreement; and
 - k) on VIIV's written request, provide VIIV with reasonable information necessary to demonstrate compliance with this clause, which may include any available third-party security audit reports.
- 3) In the event that Supplier needs to make routine transfers of VIIV Personal Information to any country, other than the country in which VIIV is established, in the normal course of business to its Affiliates and/or approved sub-processors for the provision of the Services under this Agreement, the transfer is approved by VIIV provided that the VIIV Personal Information shall be transferred and/or processed subject to: (i) the Model Clauses (as such term is defined in clause 4); or (ii) other appropriate safeguards provided by applicable Data Protection Laws and notified to VIIV in writing.

NOTE: If Supplier is based (i) outside the EEA; and (ii) in a non-Adequate country, the Model Clauses will need to be incorporated by reference as follows. Any onward data transfers of personal data will need to be considered under clause 3 above

- 4) Where VIIV (acting as a Data Exporter) transfers VIIV Personal Information to Supplier (acting as Data Importer) the parties hereby agree to abide by the EU controller to non-EU or EEA Processor model clauses approved under decision 2010/87/EU (available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=en> and incorporated herein by reference) (**Model Clauses**). To the extent of any conflict or inconsistency between any term of the Model Clauses and any other part of this Agreement, the terms of the Model Clauses shall prevail.

For the purposes of the Model Clauses:

- a. VIIV is a Data Exporter in relation to VIIV Personal Information.
 - b. Supplier, to the extent it processes VIIV Personal Information in a country outside the European Economic Area or an Adequate Country, is a Data Importer. Supplier hereby enters into this clause 4 on behalf of each Affiliate of Supplier which acts as a Data Importer.
 - c. Description of Transfers: The description of transfers, for the purposes of Appendix 1 to the Model Clauses, is set out above.
 - d. Security for Privacy: The security measures, for the purposes of Appendix 2 to the Model Clauses, are referred to in the Security Schedule.]
- 5) Where the Model Clauses are recognised as a means of implementing appropriate safeguards in relation to international transfers of Personal Data, the Model Clauses are extended to cover any other transfer of Personal Data under this Agreement.
- 6) In interpreting the Model Clauses, in countries outside of the European Economic Area, any reference to the term "Member State in which the data exporter is established" will be interpreted to mean the country in which the VIIV entity is established; and any reference to Directive 95/46/EC shall be to the law of the country where VIIV is established outside the EEA. Any reference to an **Adequate Country** shall mean any country which is held to provide, or which otherwise provides, an equivalent level of protection for the purposes of the applicable Data Protection Laws.
- 7) If any relevant supervisory authority adopts revised standard contractual clauses for the matters addressed in this Schedule (including any Annex) and VIIV notifies Supplier that it wishes to incorporate any element of those standard contractual clauses into this Schedule,

Supplier shall agree to changes as reasonably required by VIIV. In the event Supplier does not believe it can meet the requirements as reasonably set forth by VIIV, Supplier shall notify VIIV immediately of its inability and VIIV shall have the right to terminate any underlying agreement relying on this Schedule.