GENERAL TERMS FOR THE PURCHASE OF GOODS (GT)

1 DEFINITIONS AND INTERPRETATION 2
2 DELIVERY OF GOODS 5
3 LATE PERFORMANCE OR MISPERFORMANCE 5
4 TRANSFER OF OWNERSHIP AND RISK OF GOODS 5
5 WARRANTIES IN RELATION TO GOODS 6
6 ACCEPTANCE OF GOODS 6
7 SUPPLIER'S OBLIGATIONS 7
8 AUDITS AND ACCOUNTING 8
9 PRICE, INVOICING AND PAYMENTS 9
10 INTELLECTUAL PROPERTY 10
11 CONFIDENTIALITY 12
12 LIABILITY AND INDEMNITIES 12
13 INSURANCE 12
14 TERMINATION 13
15 FORCE MAJEURE 15
16 ASSIGNMENT – NOVATION 16
17 SUBCONTRACTING 16
18 TOTALENERGIES PRODUCTS 17
19 GENERAL PROVISIONS 17
20 THIRD PARTY RIGHTS 19
21 GOVERNING LAW AND DISPUTE RESOLUTION 19
22 ECONOMIC SANCTIONS AND EXPORT CONTROL 19
APPENDIX 1.1 – PREVENTION OF ILLEGAL EMPLOYMENT UNDERTAKINGS 21
APPENDIX 1.2 – ANTI-CORRUPTION UNDERTAKINGS 23
APPENDIX 1.3 – FUNDAMENTAL PRINCIPLES OF PURCHASING (FPP) 26
APPENDIX 1.4 – HYGIENE, SAFETY, AND THE ENVIRONMENT UNDERTAKINGS 29
APPENDIX 1.5 – CYBERSECURITY REQUIREMENTS 36

1 DEFINITIONS AND INTERPRETATION

1.1 DEFINITIONS

In the Contract, the following terms shall have the meanings set out below unless the context requires otherwise:

Affiliate means in relation to an entity, any other legal entity that Controls, is Controlled by, or is Controlled by an entity that Controls a Party.

Applicable Laws means all laws, ordinances, rules, regulations, by-laws, decrees, orders and the like, whether of governmental, federal, national or local authority or other agencies or other authority having jurisdiction over the Parties, the Goods, the Supplier's equipment or the Site, or any of them, and which are or may become applicable, including Sanctions Laws/ Regulations and export control laws and regulations. References to any Applicable Laws shall be construed to include a reference to that law as from time to time modified, amended, extended, re-enacted or consolidated, whether before or after the date of the Contract and any subordinate legislation made pursuant to that law.

Conform means the Goods:

(a) conform with (i) the specifications and description of the Goods pursuant to the Contract; (ii) Good Industry Practice; and (iii) any Applicable Laws, and

(b) are (i) free from defects in design, material and workmanship; and (ii) fit for any purpose specified under the Contract.

Contract means the contractual documents mutually agreed by the Parties and governing the contractual relationship between the Supplier and the Customer in respect of the Goods, including, as the case may be, the following documents and their Appendices, as per the order of precedence indicated below:

(a) the Order(s);

(b) the local implementation contract(s); and/or

(c) any other particular terms;

which refer to and incorporate directly or indirectly these General Terms ("**GT**").

(d) These GT.

In the event of a divergence or contradiction between the provisions of the documents listed above:

- any modifications to the GT must have been expressly agreed in writing;
- the body of a document shall prevail over its Appendices;
- the Mandatory Rules shall prevail over any other documents.

Control means the direct or indirect ownership of more than fifty percent (50%) of voting rights or of the registered capital, and a "**Change of Control**" is deemed to include any contribution, assignment, merger or other operation which modifies the Control, whether directly or indirectly, of the Party. Controls or Controlled shall be construed accordingly.

Customer means the individual or legal entity designated as such in the relevant Contract.

Customer Data means information and data, including personal data, the Supplier and its Personnel has access under the Contract.

Effective Date means, as the context may require, effective date of the relevant Contract.

Force Majeure means the effective occurrence of any act or event which is:

- unforeseeable;
- insurmountable;
- outside the control of the Party which invokes it; and

which renders such Party unable to comply with whole or part of its obligations under the Contract.

Provided such criteria are met all together, Force Majeure includes events such as acts of God (epidemic, tidal wave, lightning, earthquake, hurricane, flooding), war (whether declared or not), riots (other than among Supplier Personnel or Customer Personnel), civil or military disturbances, national or regional strikes (except strikes, lock-outs or other industrial disputes or actions limited to or originating with the Personnel of Supplier or its Subcontractors), any Applicable Laws (except that Sanctions Laws/ Regulations enacted after the Effective Date shall be deemed unforeseeable), and acts of any court, government or governmental authority or any representative thereof.

Good Industry Practice means any practices, methods and procedures and that degree of skill, diligence, prudence and foresight, which would reasonably be expected to be observed by a professional, skilled and experienced contractor engaged in carrying out activities the same as, or similar to, those contemplated under the Contract under the same or similar circumstances.

Goods means the goods or products or equipment (or any part of them) to be delivered by the Supplier, including, where applicable, the associated documents and the installation services of such goods or products or equipment, as defined in the Contract.

Mandatory Rules means : (a) any specific internal Site policies and procedures provided to Supplier or any member of Supplier Group by Customer in respect of a Site; (b) prevention of illegal employment undertakings (as set out in APPENDIX 1.1); (c) anti-corruption undertakings (as set out in APPENDIX 1.2); (d) fundamental principles of purchasing (as set out in APPENDIX 1.3);(e) hygiene, safety, and the environment undertakings (as set out in APPENDIX 1.4) ; and (f) Cybersecurity Requirements (as set out in APPENDIX 1.5).

Order means the documents issued by the Customer to order the supply of Goods from the Supplier. Orders can be issued electronically by the Customer to the Supplier (SAP or similar system). If a form of Order has been agreed in the relevant Contract, then Orders shall be issued in a form substantially similar to the one agreed.

Parties or **Party** means in relation to a Contract, the Customer and/or the Supplier collectively or individually.

Personnel means directors, officers, employees, agents.

Restricted Person means any individual or entity which is listed, or is 50% or more (directly or indirectly) owned, or controlled (if control is used under the relevant Sanctions Laws / Regulations) by any party listed, on a Sanctions List.

Sanctions Authority means any competent authority of: (a) the United States of America; or (b) the European Union; or (c) the Republic of France, in charge of the enactment, administration, implementation and enforcement of Sanctions Laws / Regulations.

Sanctions Laws / Regulations means any applicable economic, financial, export control or trade sanctions laws, regulations, embargoes or other restrictive measures enacted, administered, implemented and/or enforced from time to time by any Sanctions Authority or an agency thereof.

Sanctions List means any of the lists of designated sanctions targets whose assets are frozen and maintained by the Office of Foreign Assets Control of the U.S. Department of the Treasury (the specially designated nationals or blocked persons lists), by the European Union (the consolidated list of persons, groups and entities subject to financial sanctions) or the Republic of France, each such list as amended, supplemented or substituted from time to time.

Site means the location(s) where the Goods are required to be provided, as may be set out in the relevant Contract.

Subcontractor means subcontractors of any tier of Supplier performing any part of Supplier's obligations under the Contract.

Supplier means any individual or entity designated as such in the relevant Contract.

Supplier Group means Supplier and any of its Affiliates and any of their respective Personnel, or Subcontractors.

1.2 INTERPRETATION

(a) At any time and unless expressly stated otherwise, when the following expressions and description and derivatives thereof appear in any part of the Contract, they shall be construed as indicated below:

(i) "including", "included", "such as" and the like shall be deemed to be completed by the expression "but not limited";

(ii) "report", "request", "submit", "notify", "instruct", "instruction", "inform", "consent", "approve", "approval", "approved" and the like shall be deemed to be completed by the expression "in writing"; and

(iii) "property" and "equipment" shall be deemed to include property and equipment owned, operated, hired, leased or otherwise provided by the relevant person.

(b) Where the context so requires, the singular includes the plural and vice versa.

(c) Headings and table of contents are inserted only for convenience and shall not in any way limit or govern the construction of the Contract.

(d) Approval or instruction by Customer shall in no way be construed as relieving Supplier or Supplier Signatory (as the case may be) of any its obligations, responsibilities or liabilities under the Contract or otherwise.

(e) "In writing" or "written" means any communication made by letter, notice, email or through any electronic ordering or invoicing system as detailed in the Contract.

(f) References to any person, including a Party, include that person's successors in title and transferees (unless the transfer to the successor in title or transferee was in breach of the Contract). References to the Contract or any other document are references to the Contract or that other document, as varied, novated, supplemented or replaced from time to time.

(g) Each provision of the Contract shall be construed as having been negotiated by the Parties and as though all Parties participated equally in the drafting of the same. Consequently, the

Parties acknowledge and agree that any rule of construction that a document is to be construed against one of the Parties shall not be applicable to the Contract.

2 DELIVERY OF GOODS

2.1 Unless otherwise agreed by the Parties, the Goods shall be delivered at the place ("**Delivery Place**") and on the date specified in the Contract and/or the Order during normal business hours ("**Delivery Date**"). Customer shall be entitled to modify the Delivery Place and Delivery Date by prior notice to Supplier.

2.2 Any partial delivery is subject to Customer's prior written consent.

2.3 Supplier shall be responsible for packing and transporting the Goods at its own costs to the Delivery Place.

2.4 Packing shall be compliant with Good Industry Practice and appropriate for the Goods and the means of transport used to prevent any damage to the Goods during transport, handling and storage at Delivery Place. The Goods shall be duly identified and labelled by Supplier in compliance with the Contract and Applicable Laws.

3 LATE PERFORMANCE OR MISPERFORMANCE

3.1 Time is of the essence. The Supplier shall deliver Goods that Conform within the time limits and/or periods set out in the Contract. If Supplier believes it may not be able to deliver the Goods in compliance with such time limits or periods, Supplier shall immediately notify Customer and provide reasons for such delay and the appropriate corrective measures.

3.2 In addition, the Supplier is bound by an obligation to achieve a specific result and guarantees that the Goods delivered shall Conform.

3.3 Should Supplier fail to deliver the Goods by the time limits and/or periods set out in the Contract or fail to deliver Goods that Conform, Customer shall be entitled:

(a) to liquidated damages set out in the Contract,

and/or

(b) to have such Goods provided by a third party. The direct and documented costs incurred by Customer in connection with the provision of the Goods by such third party shall be payable by Supplier.

3.4 Payment of such liquidated damages shall be without prejudice to the other rights and remedies of Customer including those set out in this Clause.

The Parties agree that, where applicable, the levels of damages for delay or misperformance in this Contract represent a genuine pre-estimate of the loss that would be incurred by the Customer for the Supplier's failure to perform its obligations in accordance with the Contract.

Subject to the provisions of this Clause 3, the Supplier's total liability for late or unsatisfactory performance shall be capped as specified in the Contract.

4 TRANSFER OF OWNERSHIP AND RISK OF GOODS

Transfer of ownership

4.1 Ownership of the Goods shall transfer from Supplier to Customer on the earlier of:

(a) when the Goods can be identified as relating to the relevant Order request;

(b) when Customer pays for the Goods or part thereof in accordance with the Contract; or

(c) at the time of acceptance by Customer in accordance with the Contract.

4.2 The Goods shall be delivered free from any and all mortgages, pledges, security interests, liens, levies, charges, claims, conditions, equitable interests, options, or other encumbrance or restriction of any kind whatsoever.

Transfer of risk

4.3 The risk in the Goods shall pass to Customer as per the latest edition of the Incoterms stipulated in the Contract (or, if no Incoterm is specified, as per "Delivered Duty Paid - named place of destination" (DDP), in accordance with the latest edition of Incoterms), without prejudice to any right of rejection which may accrue to Customer under the Contract.

5 WARRANTIES IN RELATION TO GOODS

5.1 Supplier warrants that the Goods will be available for order during the term of the Contract.

5.2 Supplier warrants that the Goods shall comply in all respects with the Contract, and that they shall Conform.

5.3 Should any of the Goods not Conform within twelve (12) months from the date when such Goods are used for the first time , with a time limit of eighteen (18) months from the Delivery Date of such Goods("**Goods Warranty Period"**), Supplier shall replace, repair or rework, as directed by Customer and at Customer's sole discretion, the Goods that do not Conform , within the timeline specified by Customer with minimum disruption to Customer's operations.

5.4 Repair, replacement or rework of the Goods shall be carried out at Supplier's cost and risk, and shall include expenses and costs relating to packing, transportation to or from Supplier's manufacturing location, assistance to remove or install, and tests when necessary to confirm that such Goods Conform.

5.5 Supplier warrants the Goods, repaired, replaced or reworked in accordance with Clause 5.3 shall comply with the Contract and Conform. The Goods Warranty Period shall be extended in respect of such Goods for a duration equivalent to the period during which the Goods were being repaired, replaced or reworked or made unavailable or during which Customer's operations were interrupted, whichever lasts longer. Should any of such Goods be found not to Conform within such extended Goods Warranty Period, then Clause 5.3 shall apply.

5.6 Should Supplier fail to diligently and satisfactorily carry out the repair, replacement or rework of the Goods as provided in Clauses 5.3 to 5.5, Customer has the right, seven (7) calendar days after written notice to the Supplier, to have the replacement or rework performed by a third party upon Customer's prior notice to Supplier. The direct and documented costs incurred by Customer in connection with the repair, replacement or rework by such third party shall be payable by Supplier. Repair, rework or replacement by a third party under this Clause shall not relieve Supplier from its warranty obligations under the Contract.

5.7 The warranties under this Clause 5 shall not apply to the extent that Supplier demonstrates that repair, replacement or rework of the Goods results from: (a) normal wear and tear; or (b) damage caused by a third party, or by a Customer's misuse, unless such damage or misuse is due to acts, omissions, faulty instructions or negligence of any member of Supplier's Group.

6 ACCEPTANCE OF GOODS

6.1 Acceptance of Goods will be declared by Customer: (i) when the Customer has inspected such Goods to see whether they Conform, and (ii) if the Goods are Conform and all elements of the Goods as described in the Contract have been provided to Customer.

6.2 Acceptance of delivery and/or payment, in whole or in part, of the Goods by Customer does not entail acceptance of the Goods. Acceptance of the Goods (with or without reserve), or refusal to accept the Goods, must be recorded in a written document.

Acceptance without reserves

Acceptance without reserve shall occur when Customer confirms in writing that it accepts the Goods without reserves.

Non-Conformity during acceptance

Should Customer identify Goods that do not Conform, then Customer has the right to either:

(a) accept such Goods with reserve(s), in which case Supplier shall carry out the repair, replacement or rework necessary to remedy the reserves within the period given by Customer.

If at the end of this period, Supplier has not satisfactorily carried out the repair, replacement or rework, Customer may either:

(i) terminate the Contract, in accordance with the Clause "Termination due to Supplier's default"; or

(ii) apply a proportionate reduction in the price(s) payable for the relevant Goods; in any case, Customer shall be entitled to liquidated damages pursuant to Clause 3.

(b) refuse acceptance and postpone the date of acceptance by sending notice of postponement to Supplier, indicating a deadline for a new inspection of Conformity;

or

(c) refuse acceptance and terminate the Contract in accordance with Clauses 14.1, 14.2, and 14.3.

6.3 The Supplier shall remain fully responsible for any defects or for any non-Conformity whatsoever which were not apparent at the time of acceptance despite acceptance by the Customer, which, in any case shall not reduce or otherwise affect Supplier's obligations and warranties under the Contract.

7 SUPPLIER'S OBLIGATIONS

General

7.1 Supplier shall, and shall ensure that its Personnel, its Subcontractors and their Personnel perform the Contract:

(a) in accordance with the time schedule set out in the Contract, and, if not specified, then promptly;

(b) in compliance with Good Industry Practices, any Applicable Laws, and Mandatory Rules;

(c) by exercising all care, skill and diligence to prevent damage to Customer's Site or property; and

(d) as an independent contractor and neither Supplier nor any of its Subcontractors nor any of their Personnel shall be deemed for any purpose to be Customer's Personnel.

Duty to inform

7.2 Supplier shall ensure it is aware of:

(a) any foreseeable external factors and conditions (including but not limited to technical conditions); and

(b) any risks connected with the Goods, including but not limited any hygiene, safety and environmental risk,

that may affect the performance of the Contract and shall inform Customer and provide any advice mitigating such factors, conditions or risks regardless of Customer's knowledge or expertise.

Careful examinations of Customer information

7.3 Supplier shall carry out a careful examination of information provided by or on behalf of Customer for the provision of Goods, including any updated versions of any Mandatory Rules, and Supplier shall inform Customer of any anomalies or omissions.

Customer shall not be liable for the accuracy and completeness of such information.

Authorisations

7.4 Supplier warrants that it and its Subcontractors shall, in compliance with Applicable Laws, maintain at their own costs during the term of the Contract all statutory registrations, approvals and authorisations granted by public authorities or professional organisations required to perform its obligations under the Contract ("**Authorisations**"). Customer has the right to request Supplier to provide evidence of Authorisations prior to the commencement of any provision of Goods. In the event, any Authorisation becomes invalid for any reason whatsoever, Supplier shall immediately inform Customer of the same and Customer shall be entitled to terminate the Contract in accordance with Clause 14.

Personnel

7.5 The Supplier undertakes to assign a Personnel who is qualified, authorized and free from any conflict of interest to perform the Services, to ensure their availability and cooperation throughout the duration of the Contract, while retaining hierarchical authority and control over such Personnel.

Return or destruction of Customer Data

7.6 Unless otherwise specified in the Contract, the Supplier undertakes to return or destroy all or part of the Customer Data:

(a) at any time upon written instruction from the Customer; or

(b) upon expiry or termination of the Contract for any reason whatsoever, within 30 calendar days of receiving written instruction from the Customer.

8 AUDITS AND ACCOUNTING

8.1 Subject to eight (8) days prior notice to Supplier, Customer is entitled, at any time, to ensure that Supplier or its Subcontractors comply with their obligations under the terms of the Contract by carrying out itself or by a third party, remote audits of Supplier or its Subcontractors or at their respective facilities ("**Audits**").

Supplier shall provide Customer with all assistance necessary for conducting such Audits. Information obtained during any Audit shall not be used for any purpose other than such Audit. Customer has the right during any Audits to copy any records and accounts for verification of any sum payable under the Contract.

8.2 Such Audit shall not reduce or otherwise affect:

(a) Supplier's obligations, liabilities and warranties under the Contract,

(b) Supplier's status of independent contractor as provided in Clause 7.1(d), and

(c) Customer's right to refuse any Goods.

8.3 Supplier shall safely keep, and cause its Subcontractors to keep, in accordance with generally accepted accounting practice, accurate detailed records and accounts relating to the Contract for an accurate audit and verification of any reimbursable costs, for the duration of the Contract and for a period of two (2) years from its termination or expiry.

8.4 Should the audit report show any non-compliance by Supplier with its obligations under the Contract, the latter agrees to implement, at its own cost, the necessary remedial measures within a period compatible with the criticality of the non-conformities identified.

9 PRICE, INVOICING AND PAYMENTS

Payment, price and taxes

9.1 In consideration for the provision of the Goods, Customer shall pay Supplier the prices as specified in the Contract. Such prices are fully inclusive of all cost, firm and non-revisable, and shall include all taxes other than VAT.

9.2 Supplier shall be solely responsible and liable for all taxes, imposts, levies, fees, stamps, customs duties and dues of any kind which may be assessed or levied by whatsoever authorities on Supplier ("**Taxes**"), its Affiliates, Subcontractors and Personnel in any country in connection with the performance of the Contract, including any taxes which Customer may be obligated to withhold from its payments to Supplier in accordance with Applicable Laws.

9.3 Supplier shall defend, indemnify and hold Customer and its Affiliates harmless from and against any claim, demand, cause of action, proceedings, judgements, award (including reasonable legal fees, costs and expenses and sums paid by way of settlement), liability, loss, expense, penalty, fine and damages and the like for Taxes arising from, relating to, or in connection with the performance, mis-performance or non-performance of the Contract and for which Supplier is responsible in respect of Clause 9.2. Supplier represents that, in setting its prices for the supply of the Goods under the Contract, it has taken into account all Taxes for which it is liable in accordance with this Clause.

Invoicing

9.4 Supplier shall issue invoices to be sent to Customer's address and in the currency specified in the Contract. Such invoices shall comply with the Contract (including APPENDIX 1.2 of the GT), any other instruction of Customer and Applicable Laws.

9.5 Upon Customer's request, Supplier shall set up an electronic invoicing system, using a platform specified by Customer. Each Party shall enter into an agreement with such provider.

9.6 In addition to the requirements of Applicable Laws, invoices shall contain the following information:

- Supplier's EU VAT code if any;
- references or identification number of the Contract;

- the period for which the invoice relates;
- the amounts due by Customer;
- the basis on which the amounts due have been calculated;
- the description and quantity of all Goods provided;
- the nomenclature, the net weight in kilograms, the transportation mode and the country of origin of the Goods;
- if necessary, copies of documentation in support of the amounts invoiced; and
- the relevant Order reference number.

9.7 Customer shall pay non-disputed invoices by means of electronic transfer of funds (or other agreed method) within thirty (30) days from the last day of the month in which the invoice was issued.

9.8 Any undisputed invoice due and payable by Customer shall bear interest thereon from the due date of such invoice, calculated:

(a) for invoices governed by the mandatory French laws on payment term, at the rate equal to three times the French legal interest rate in effect in France; or

(b) for any other invoices, at the average rate (for the period of delayed payment) of the last three (3) months European Inter Bank Offered Rate (as published by the Banque de France) or its substitute as may be agreed by the Parties, plus one percent (1%).

Disputed invoices

9.9 In the event Customer disputes all or part of an invoice, Customer shall send a notice to Supplier specifying the reasons for its refusal to pay. Customer shall have no obligation to pay any disputed amount until such dispute is resolved between the Parties; in that case, Supplier shall correct the invoice and submit it to Customer for payment in accordance with this Clause 9.

Offset

9.10 Customer shall have the right at its sole discretion to offset amounts owed by Supplier against amounts payable by Customer under the Contract.

10 INTELLECTUAL PROPERTY

Specific Elements

10.1 In consideration for Customer's payment of the price specified in the Contract, Supplier shall assign to Customer, and warrants the assignment by its Personnel, its Subcontractors and their Personnel of all intellectual property rights relating to any specific elements provided to comply with Customer's specifications, including but not limited to plans, studies, models, designs and drawings, user guides, technical documentation, manuals, and documents ("**Specific Elements"**).

10.2 The assignment as provided in Clause 10.1 shall occur when such Specific Elements are created and shall be exclusive, world-wide, perpetual, royalty-free, transferable, and shall include all rights to exploit such Specific Elements: the rights of reproduction, representation, translation, adaptation and sale, on all media and for all forms of use and exploitation.

Standard elements

10.3 In case the Goods contain standard elements, which are not developed specifically for Customer or any of its Affiliates, protected by intellectual property rights (including but not limited to standard plans, manuals, documents and software), delivered to Customer by Supplier, in consideration for the remuneration included in the price specified in the Contract, Supplier grants Customer, any of

its Affiliates that may be beneficiaries of the Contract and third parties acting on behalf of Customer, a personal and non-exclusive, royalty-free, worldwide, perpetual, transferable right to use, reproduce, represent, translate, repair and adapt such standard elements for the needs of Customer and any of its Affiliates.

10.4 In case of transfer by Customer to a third party of any equipment or any material or asset, which embodies or uses a standard element, the above Customer's right to use shall be transferred to such third party at no additional cost.

10.5 Each Party retains all the rights it holds on the methodologies and analysis methods, know-how and experience acquired prior to the Contract, provided, in relation to Supplier, that these do not include Specific Elements.

Acquisition of third party rights

10.6 Supplier shall be responsible for acquiring all authorizations and intellectual property rights from third parties required for performance of the Contract, including from its employees and Subcontractors. Notably, should the performance of the Contract comprise the use of one or more software programs owned by a third party, Supplier shall procure, at its own cost, for Customer and third parties involved in the Contract, the non-exclusive right to use such third-party software in the scope of the Contract.

Infringement of intellectual property rights and other third party's rights

10.7 Supplier warrants that it and its Subcontractors, is either the owner of all intellectual property rights relating to any delivered elements or that it has been granted all necessary licences and authorisations from third parties owning intellectual property or exploitation rights, to enable Customer to freely use and exploit such elements in accordance with the provisions of this Clause 10.

Supplier shall and shall ensure that its Personnel and Subcontractors shall not infringe or cause Customer to infringe any third party's rights, in particular infringement of their intellectual property rights. This warranty shall not apply if Supplier can demonstrate that the infringement alleged is attributable to Customer.

10.8 Supplier shall indemnify and hold Customer harmless from and against any and all claims, costs, damages, expenses or legal action by third parties arising out of or in connection with any infringement or any other breach of their rights.

10.9 In the event of a risk of a claim or legal action, Supplier shall take all steps necessary to ensure that the risk of infringement is eliminated, shall inform Customer thereof and shall take into account Customer's business constraints.

10.10 In case an allegation is made that Customer may not use an element which forms part of any Goods without infringing a third party's right, Supplier shall, at its own cost and at the sole option of Customer, either replace the element in respect of which such allegation is made, or modify such element so that the infringement or any other breach no longer exists, in compliance with the specifications applicable to such element. Such replacements or modifications shall be performed within periods compatible with Customer's needs. Should Supplier fail to make such replacements or modifications, Supplier shall reimburse Customer for the price of such Goods.

10.11 The above provisions do not affect the Customer's right to claim damages from the Supplier and/or terminate the Contract in accordance with the provisions of Clause 14.

11 CONFIDENTIALITY

11.1 All information or data provided by one of the Parties to the other Party shall be considered confidential, except if such information is already or falls in the public domain without breach of Contract, and except if it has been lawfully obtained by a Party from any third party having the right to disclose such information.

11.2 The receiving Party may not disclose such information and data to any other person except as provided in this clause or as may be required to be disclosed under Applicable Laws.

11.3 Supplier undertakes to restrict access to such information and data to those members of its Personnel, its Affiliates and its Subcontractors who need it for the performance of the Contract and who are bound by confidentiality undertakings at least equivalent to those stipulated under the terms of this clause.

11.4 Customer undertakes to restrict access to this information and data to:

(a) members of its Personnel,

(b) its Affiliates,

(c) and, provided that they are bound by confidentiality undertakings at least equivalent to those stipulated under the terms of this clause:

(i) its partners or prospective or future partners that have a need to know,

(ii) *bona fide* prospective transferees of a Customer's interest to the extent appropriate in order to allow the assessment of such interest

(iii) third parties acting on behalf of or for the needs of the Customer, its Affiliates, or the partners mentioned above.

11.5 Supplier undertakes not to refer to or use Customer's trade name or registered trademarks for any reason whatsoever without having first obtained the Customer's express written authorisation.

12 LIABILITY AND INDEMNITIES

12.1 Each Party shall:

(a) be liable for any damage (including any injuries, death, damage to or loss of property) that

(i) it, its Personnel, and with respect to Supplier, any Subcontractors cause to the other Party or to a third party; and/or

(ii) is arising out of or in connection with the performance, misperformance or non-performance of the Contract (whether caused by negligence, breach of statutory duty, tort, willful misconduct or other fault); and

(b) defend, indemnify and hold harmless the other Party and its insurers from and against any damage, cost and/or liability that the other Party may suffer in this respect.

13 INSURANCE

13.1 Supplier shall take out and maintain in force, at its own costs, during the performance of the Contract, necessary insurance policies in accordance with Good Industry Practices, and shall procure that its Subcontractors do the same. The insurance amounts indicated below are minimum requirements and not limits of liability.

Insurance product & coverage	Minimum coverage
General and public liability / third party liability	2 500 000 € combined single limit, per occurrence
Products liability or Professional Liability insurance	2 500 000 € per occurrence
A worker's compensation insurance covering damages caused to its (their) Personnel, when the Supplier and/or the Subcontractors is located in a country in which there is no system of social security insurance	« *To be determined* »
Employer's legal liability insurance policy	2 500 000 € per occurrence
An Automobile Public Liability Insurance (whenever automobiles and automotive equipment are employed by Supplier for the performance of the Contract)	1,000,000 € per occurrence
Any other insurance policies mandatory in the country of the Site	« *To be determined* »

13.2 Prior to supplying the Goods and at each insurance policy's renewal required throughout the duration of the Contract, Supplier shall provide Customer with the certificate(s) issued by its insurer in accordance with the amounts defined as above.

13.3 If, and to the extent applicable, each Party's insurances shall contain provisions whereby the insurers waive their rights of subrogation against the other Party and its Affiliates and their respective insurers to the extent of the liabilities and indemnities assumed by the other Party under the Contract.

14 TERMINATION

Termination due to Supplier's default

14.1 Customer shall be entitled to terminate as of right all or any part of the Contract in the event of a breach of an obligation by the Supplier that is not remedied within fifteen (15) calendar days after receipt of a written notice to do so. In particular, the Customer shall be entitled to terminate all or any part of the Contract in the event of default or breach or failure relating to Supplier's obligation to deliver Goods that Conform.

14.2 Notwithstanding Clause 14.1, Customer shall have the right to terminate all or part of the Contract forthwith in the following cases:

(a) A series of breaches by Supplier, as set out in Clause 14.1

(b) A breach by Supplier, the consequences of which is not capable of being remedied, such as non-compliance with Clause 3, Clause 7.4 and Clause 11;

(c) Customer becomes aware that Supplier will be unable to provide the Goods by the Delivery Date;

(d) where applicable, the master and/or local implementation contract the Contract is implementing has been terminated by the relevant Customer for any of the reasons provided in this clause 14,

(e) Non-compliance by Supplier with Applicable Laws and/or Mandatory Rules.

Such termination shall be effective on the date indicated in the notice of termination or, otherwise, on the date of receipt by Supplier of the notice of termination.

14.3 In case of termination of the Contract in accordance with Clause 14.1 or 14.1:

(a) Customer shall only be liable to pay Supplier, as full and final compensation under the Contract or otherwise, the amount due for Goods delivered in Conformity by the Supplierprior to the date of termination, and accepted by Customer; and

(b) Customer is entitled to have all or part of Supplier's outstanding obligations under the Contract performed by another supplier and to invoice Supplier for the difference in price between (i) the cost incurred by Customer; and (ii) the cost Customer would have incurred if Supplier had fully performed the Contract, and Customer shall be entitled to all direct and documented costs,damage and expenses (including additional managerial expenses and administrative services) suffered by Customer in connection with such termination; and

(c) any monies due to Customer pursuant to this Clause 14.3 shall be paid to Customer within thirty (30) days from the last day of the month in which the invoice was issued, failing which such outstanding amounts shall accrue interest at the rate specified in Clause 9.8 from the due date of such invoice until the date that such outstanding amounts are paid in full.

Termination due to Change of Control or insolvency of Supplier

14.4 Without prejudice to any other rights under the Contract, Customer may terminate the Contract at any time after notice if Supplier is the subject of any of the following events or circumstances:

(a) unless contrary to any statutory provision of public order, if Supplier is the subject of any of the following events or circumstances:

(i) it is unable to pay its debts as they fall due or admits inability to pay its debts;

(ii) it stops or suspends, or threatens to stop or suspend, making payments with respect to all or any class of its debts or it suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

(iii) it makes a proposal for or enters into any compromise or arrangement with its creditors other than for the sole purpose of a scheme for a solvent amalgamation with one or more other companies or a solvent reconstruction;

(iv) a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with its winding up other than for the sole purpose of a scheme for a solvent amalgamation with one or more other companies or a solvent reconstruction;

(v) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is given or if an administrator is appointed, over it;

(vi) a person becomes entitled to appoint a receiver over its assets or a receiver is appointed over its assets; or

(vii) any event occurs, or proceeding is taken, with respect to it in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in (i) to (vii) (inclusive).

(b) Supplier undergoes a Change of Control.

In case of termination due to Change of Control or insolvency of the Supplier, provisions of Clause 14.3 will apply.

Termination at Customer's convenience

14.5 Without prejudice to the other provisions of the Contract, Customer may at its discretion terminate all or part of the Contract at any time by serving notice but shall in such case:

(a) pay Supplier the amount due for Goods delivered in Conformity by Supplier prior to the date of termination and accepted by Customer;

(b) reimburse Supplier for all costs reasonably and irrevocably incurred and paid or committed in good faith as evidenced by supporting documents in respect of the Goods ordered but not delivered on such termination;

(c) pay Supplier five per cent (5%) of the difference between (i) the price Supplier would have received for full performance of the Contract, including any outstanding or partially performed Order, and (ii) the aggregate of the amounts already paid to Supplier in accordance with Clause 14.5(a) and 14.5(b).

14.6 Such payments in accordance with Clause 14.5 shall constitute the full and final compensation payable by Customer to Supplier under the Contract and Supplier shall have no claim against Customer for such termination.

Termination for prolonged Force Majeure event

14.7 Without prejudice to any other provisions of the Contract, Customer may terminate the Contract at any time by serving notice if an event of Force Majeure continues for more than thirty (30) days.

14.8 If Customer terminates the Contract in accordance with Clause 14.7, Customer shall (a) pay Supplier the amount due for Goods delivered by Supplier and accepted by Customer prior to the date of termination; and (b) reimburse Supplier for all costs reasonably and irrevocably incurred and paid or committed in good faith as evidenced by supporting documents in respect of the Goods ordered but not delivered on such termination.

14.9 Such payments in accordance with Clause 14.8 shall constitute the full and final compensation payable by Customer to Supplier under the Contract and Supplier shall have no claim against Customer for such termination.

15 FORCE MAJEURE

15.1 None of the Parties shall be deemed to be in breach of its contractual obligations for any delay in performance of, or for any failure to perform, any obligation, in whole or in part, under the Contract to the extent that this delay, non-performance or failure results from or is due to Force Majeure. Force Majeure shall only relieve the affected Party from its obligations under the Contract to the extent and for such period as the said Party is prevented or delayed from performing its obligations. Each Party shall bear all its own expenses resulting from the occurrence of Force Majeure.

15.2 The affected Party shall immediately notify the other Party in writing. Such notice shall include:

(a) details of the occurrence and nature of the relevant act, event or circumstance claimed by it to constitute Force Majeure; and

(b) an estimate of the duration such act, event or circumstance is likely to persist in respect of its obligations affected (if possible).

15.3 Any Party whose obligations have been suspended under the foregoing provisions of this Clause 15 shall:

(a) notify the other Party as soon as practicable after the Force Majeure event has ceased;

(b) resume performance of its obligations under the Contract as soon as reasonably practicable;

(c) use reasonable endeavours to remedy the situation as quickly as possible; and

(d) notify the other Party when such resumption is expected to occur and when it does occur.

16 ASSIGNMENT – NOVATION

16.1 No member of the Supplier Group shall assign, novate or otherwise transfer its rights and obligations under a Contract to any third party, in whole or in part, without the prior written consent of the relevant Customer. The assigning party shall remain jointly and severally liable with its assignee towards the relevant Customer for the full performance of the relevant Contract.

16.2 Customer shall be entitled to assign, novate or otherwise transfer its rights and obligations under the Contract to any of its' Affiliates, upon notice to Supplier.

In the event of a Change of Control of the Supplier, the Supplier shall promptly inform the Customer.

Transfer of an Affiliate, an asset, or a business operation

16.3 In the event an Affiliate, an asset, or business operation is removed from the scope of the Customer (the "**Transferred Entity**") due to a total or partial spin-off, divestiture of shares or business operations, merger, Change of Control, the Transferred Entity may no longer place any Order as of the date of effective departure of the Assigned Entity from the Customer.

16.4 The delivery of the Goods in progress shall automatically end on that date. Supplier shall reimburse pro rata temporis any payments already made in respect of such delivery in progress that have not been performed on the effective date of departure. Supplier shall have no claim in respect of the end of such Orders on this basis.

16.5 However, if so requested, Supplier hereby agrees to continue to deliver the Goods in progress for the benefit of the Transferred Entity during a period necessary to maintain the activities of the Transferred Entity.

17 SUBCONTRACTING

17.1 Except as provided in this Clause 17, and unless Customer has duly preapproved one or several Subcontractors for the performance of part of the Supplier's obligations under the relevant Contract, the latter shall not subcontract any of its obligations under the Contract.

17.2 Should Supplier wish to subcontract part of its obligations under the Contract, it shall send a prior written request to Customer specifying (a) any details regarding the proposed Subcontractor including any relevant qualifications; and (b) the obligations under the Contract that Supplier wishes to subcontract.

17.3 Supplier shall prohibit its own Subcontractors from subcontracting any obligations under the Contract, except as approved by the Customer.

17.4 Supplier shall be responsible for the performance of its Subcontractors in accordance with the Contract. Supplier shall defend, save, indemnify and hold Customer harmless from and against any consequences arising from Subcontractors' non-compliance with the requirements of the Contract and any claim made by its Subcontractors, their suppliers or their respective Personnel.

18 TOTALENERGIES PRODUCTS

As far as legally permissible, Supplier shall, in the performance of the Contract, procure and use, and require that its Subcontractors procure and use, products and services marketed by Customer or any of its Affiliates, including marine, road and aviation fuels, base oils, drilling fluids and well services, solvents, natural gas and electricity, greases, lubricants, additives, polymers, chemicals, seals and valve components, battery systems and photovoltaic systems, subject to availability and provided that prices are competitive. If Supplier cannot procure, use or specify the use of such products, Supplier shall so inform Customer and justify its reasons.

19 GENERAL PROVISIONS

19.1 *Notices and delivery*

(a) Any notices given under the Contract shall be in writing and in English, delivered by hand, by registered letter with acknowledgement of receipt, by courier using an internationally recognised courier company if sent abroad, or by electronic mail with proof of receipt, to the postal address or electronic address, specified in the Contract. A Party may change its postal address, electronic address and/or details by prior notice to the other Party in accordance with this Clause 19.

(b) A notice shall be treated as having been received:

(i) at the time of delivery, if delivered by hand, by registered letter with acknowledgement of receipt or courier;

(ii) at the time of receipt by the sender of a proof of receipt by the addressee, if transmitted by electronic mail.

19.2 *Severability*

If any provision of the Contract is deemed invalid by a court or any other competent authority for any reason, such invalidity shall not affect the validity or operation of the other provision of the Contract except only so far as shall be necessary to give effect to the construction of such invalidity and any such invalid provision shall be deemed severed from the Contract without affecting the validity or the balance of the Contract.

19.3 *Waivers*

The failure on the part of either Party to enforce, from time to time, all or any portion of the terms and conditions of the Contract shall not constitute a waiver of such terms or conditions.

19.4 *Entire agreement*

The Contract constitutes the entire agreement between the Parties, and supersedes all prior oral and written negotiations, understandings, representations and/or agreements with respect to the Contract made between the Parties prior to the Effective Date.

19.5 *Cumulative rights*

The rights and remedies of the Parties shall not be limited to those set out in the Contract, and such rights and remedies shall be cumulative, and are not exclusive of any other rights or remedies provided by the Contract, law, equity or otherwise, provided however that the Contract shall always take precedence over any Applicable Laws with which it conflicts, or which are expressly excluded by the Contract as far as legally permissible. Except as expressly stated in the Contract (or in law or equity), in the case of rights and remedies provided by law or equity, any right or remedy may be exercised wholly or partially from time to time.

19.6 *Liens*

The Supplier shall not create or do anything (including by act, omission or negligence) which would result in the creation of any lien or charge on the Customer's Site, property and equipment and/or the Goods or any part thereof. The Supplier hereby represents that it has not created any such lien or done anything as above before entering into the Contract.

The Supplier shall defend, indemnify and hold the Customer harmless from and against any lien with respect to Customer's Site, property and equipment and/or the Goods or any part thereof, if directly created or caused by act, omission or negligence of the Supplier's Group.

19.7 *Amendments*

No modification of the Contract shall be effective unless set out in a written amendment duly signed by authorised representatives of the Parties.

19.8 *Surviving clauses*

(a) Termination or expiry of the Contract for any reason shall not affect any rights or liabilities that may have accrued prior to such termination or expiry.

(b) Without prejudice to the generality of Clause 19.8(a), any provision of the Contract which is intended to apply after termination of the Contract shall survive the termination of the Contract for whatever reason and shall continue notwithstanding such termination and thereafter remain in full force and effect.

19.9 *Further assurance*

Supplier shall at its own cost do and/or execute or arrange for the doing and/or execution of, any act and/or document reasonably requested of it by Customer to implement and give full effect to the terms of the Contract.

19.10 *Counterparts*

The Contract may be entered into in any number of counterparts and by the Parties on separate counterparts, all of which taken together shall constitute one and the same instrument.

19.11 *Relationship of Parties*

The Contract has been concluded between independent Parties. No provisions of the Contract shall be interpreted as giving the right or mandate to either Party to act on behalf of the other Party and does not authorise any Party to bind any other Party nor as implying any association, agency, partnership, relationship of principal and agent or society between them, or as creating a joint and several liability between them.

19.12 *No exclusivity*

No provision of the Contract shall be deemed to confer any exclusivity in favor of Supplier.

19.13 *No joint and several liability*

There will be no joint and several liability between Customer, on the one hand, and any of its respective Affiliates on the other hand. Consequently, each Affiliate of Customer shall remain solely responsible for the performance of its obligations towards the relevant Supplier.

20 THIRD PARTY RIGHTS

20.1 Each of Customer's Affiliates (as applicable) shall have the benefit of all rights, benefits and limitations provided for in the Contract and accordingly shall be entitled to enforce and rely on the Contract as if it were a Party.

20.2 Notwithstanding Clause 20.1, Customer and Supplier may agree to rescind or vary the Contract without the consent of any other person or entity.

20.3 Except as provided in Clause 20.1 and in any particular terms, the Contract is intended to be solely for the benefit of the Parties and is not intended to confer any benefits upon, or to create any rights in favour of, any person other than the Parties.

21 GOVERNING LAW AND DISPUTE RESOLUTION

21.1 The interpretation, existence and validity of the Contract shall be subject to the laws of England and Wales.

21.2 Except as specified in the Contract, the Parties agree to submit any dispute to the exclusive jurisdiction of the courts of England and Wales.

21.3 The Parties expressly waive the application of the United Nations Convention on contracts for the international sale of goods (CISG).

22 ECONOMIC SANCTIONS AND EXPORT CONTROL

22.1 Supplier represents and warrants that, as of the Effective Date:

(a) no Sanctions Laws / Regulations hinder or prevent Supplier Group from executing the Contract;

(b) none of Supplier, its Affiliates (to the extent they are involved in the execution of the Contract), its Subcontractors and its and their shareholders and directors is a Restricted Person, and

(c) Supplier possesses or will possess the authorizations and licenses required to import and/or export Supplier's equipment or any other goods, equipment and technology used or supplied for the execution of the Contract in compliance with Sanctions Laws/ Regulations and applicable export control laws and regulations.

22.2 Notwithstanding any other provision in the Contract, in no event shall either Party be obligated to perform any of its obligations under the Contract, including payment, that would result in a breach, or violation of Sanctions Laws/ Regulations, or subject a Party or any of its Affiliates to punitive measures thereunder (a "**Sanctioned Obligation**").

22.3 If a Sanctions Laws/ Regulations constitutes Force Majeure:

(a) the Party whose performance is so affected ("**Affected Party**") shall as soon as reasonably practicable issue the notice required as set forth in Clause 15, which notice shall contain the following minimum information: (i) an identification of the Sanctions Laws/ Regulations that is considered to constitute Force Majeure, and description of the relevant Sanctioned

Obligation (ii) the extent to which the Affected Party is prevented from performing the Contract, and

(b) either Party may:

(i) suspend the Sanctioned Obligation or

(ii) terminate the Contract

as set forth in Clause 15 or in Clause 14.7, 14.8 and 14.9.

(c) In the event of a partial suspension as set forth in this Clause 22.3 (b)(i), the Affected Party shall continue to perform its obligations under the Contract to the extent that they are not Sanctioned Obligations.

22.4 Notwithstanding anything to the contrary in this Contract, should Supplier be in breach of Sanctions Laws/ Regulations or otherwise unable to perform its obligations under the Contract due to a Sanctioned Obligation that does not amount to Force Majeure, then Customer shall have the right to terminate the Contract forthwith by giving written notice to the Supplier. Such termination shall be effective from the date of receipt of the notice and the consequences of such termination shall be those set forth in Clauses 14.1, 14.2 and 14.3.

22.5 Either Party may request from the other Party any information required by a Sanctions Authority, in which case such Party shall duly comply with such request unless such information is covered by privilege, or confidentiality.

22.6 Supplier shall perform and update due diligences on its Subcontractors using reputable screening tools such as World-Check to ensure compliance with Sanctions Laws/ Regulations and Customer reserves the right to request proof of and/or documentation relating to such due diligences.

22.7 Supplier shall promptly notify Customer if any member of the Supplier Group or any of its or their shareholders or directors become a Restricted Person.

APPENDIX 1.1 – PREVENTION OF ILLEGAL EMPLOYMENT UNDERTAKINGS

Supplier registered in France

1 Supplier garantit, dans le cadre du présent Contrat, la régularité de sa situation au regard de la législation sociale. A ce titre, Supplier certifie avoir procédé aux déclarations exigées par les organismes de protection sociale et avoir rempli les obligations indiquées aux articles L.8221-3 et L.8221-5 du Code du Travail.

2 Supplier s'engage à remettre à la signature du Contrat puis tous les six mois à compter de cette date, les documents mentionnés ci-dessous, conformément aux articles D.8222-5, D.8222-7 et D.8222-8 et aux articles D.8254-2 et suivants du Code du travail:

3 Dans tous les cas :

3.1 Une attestation de fourniture de déclarations sociales et de paiement des cotisations et contributions de sécurité sociale prévue à l'article L. 243-15 du Code de la sécurité sociale émanant de l'organisme de protection sociale chargé du recouvrement des cotisations et des contributions sociales incombant au Supplier datant de moins de six mois, et

3.2 Cette attestation devra permettre la vérification de son authenticité auprès dudit organisme, au moyen du dispositif d'authentification prévu à l'article D. 243-15 du Code de la sécurité sociale.

4 Lorsque l'immatriculation au répertoire des métiers ou au registre du commerce et des sociétés est obligatoire :

4.1 Un original de l'extrait de l'inscription au registre du commerce et des sociétés (K ou K bis) datant de moins de trois mois, ou

4.2 Une copie de la carte d'identification justifiant l'inscription au répertoire des métiers, ou

4.3 Un devis, document publicitaire ou correspondance professionnelle mentionnant le nom ou la dénomination sociale, l'adresse complète et le numéro d'immatriculation au registre du commerce et des sociétés ou au répertoire des métiers ou à une liste ou un tableau d'un ordre professionnel ou la référence à l'agrément délivré par l'autorité compétente, ou

4.4 Un récépissé du dépôt de déclaration auprès du Centre des Formalités des Entreprises pour les personnes en cours d'inscription.

5 Lorsque le Supplier emploie des salariés étrangers et soumis à l'autorisation de travail mentionnée à l'article L.5221-2 du Code du travail :

5.1 Une liste nominative des salariés étrangers et soumis à l'autorisation de travail mentionnée à l'article L.5221-2 du Code du travail, cette liste mentionnant, pour chaque salarié, sa date d'embauche, sa nationalité ainsi que le type et le numéro d'ordre du titre valant autorisation de travail.

Supplier not registered in France

6 Supplier shall produce the documents and attestation listed below at the signature of Contract. Whenever whole or part of the Services are to be performed in France, Supplier shall reiterate the provision of said documents and attestation every six (6) months until the end of the Term.

7 These documents and certificates should be written in the French language or sent along with a translation into French.

8 In all cases:

8.1 a document quoting its individual identification number or, if Supplier is not held to have such a number, a document stating its identity and address or, as the case may be, the details of its tax representative in the country of operations; and

8.2 should it be required by the legislation of the state where Supplier has its registered address, a document established by the body in charge of monitoring the compulsory social/labour scheme relevant to Supplier and certifying that Supplier has performed the mandatory social declarations and the payment of its associated contributions, and

8.3 Whenever whole or part of the Services are to be performed in France:

(a) a document testifying to Supplier's regular social/labour status with respect to regulation (CE) n°883/2004 as of 29th April 2004 or to an international social/labour security convention, or

(b) a certificate of social declaration and payment of social contributions and taxes as provided for by article L. 243-15 of the French Social Security Code. In such a case, this certificate shall be in a way to allow the verification of its authenticity through the authentication system provided for by article D. 243-15 of the French Social Security Code.

9 When Supplier's registration with a trade registry is mandatory in the country of operation or domiciliation:

9.1 a document issued by the authorities in charge of keeping said trade registry or a document testifying to such registration; or

9.2 a bill of quantities, advertising document or trade correspondence, mentioning the name or corporate title, full address and nature of registration to the trade registry; or

9.3 for companies in the process of incorporation, a document less than six (6) months old from the organisation entitled to receive registration to the trade registry and testifying to the registration application for said registry.

10 When Supplier seconds on the French national territory foreign employees subject to the work authorisation provided under article L.5221-2 of the French Labour Code as part of performance of Contract:

10.1 a name list of the foreign employees subject to the work authorisation provided under article L.5221-2 of the French Labour Code, should mention, for each single employee, their hiring date, nationality as well as the type and order number of work authorisation document.

APPENDIX 1.2 – ANTI-CORRUPTION UNDERTAKINGS

1 DEFINITIONS

CLOSE FAMILY MEMBER OF A PUBLIC OFFICIAL means a husband/spouse or partner, one of their children, siblings or parents; the husband/spouse or partner of their children or siblings; or any household member.

PUBLIC OFFICIAL means an elected or appointed official, employee or agent of any national, regional or local government/state or department, agency or instrumentality of any such government/state or any enterprise in which such a government/state owns, directly or indirectly, a majority or Controlling interest; an official of a political party; a candidate for public office; and any official, employee or agent of any public international organization.

2 PREVENTION OF CORRUPTION

2.1 In recognition of the principles enshrined in the pertinent international and regional conventions on combating corruption and to ensure compliance with the anti-corruption laws applicable to the activities under the Contract and any other anti-corruption laws otherwise applicable to the Parties or their ultimate parent company,

2.2 Supplier, in respect of the Contract and the matters that are the subject of the Contract, warrants that neither it nor to its knowledge anyone on its behalf, has made or offered nor will make or offer any payment, gift, or promise or give any advantage, whether directly or through an intermediary, to or for the use of any Public Official, where such payment, gift, promise or advantage would be for purposes of:

(a) influencing any act or decision of such Public Official;

(b) inducing such Public Official to do or omit to do any act in violation of their lawful duties;

(c) securing any improper advantage; or

(d) inducing such Public Official to use their influence to affect any act or decision of any department, agency or instrumentality of any government or public enterprise.

2.3 Supplier, in respect of the Contract and the matters that are the subject of the Contract, warrants that it has not made or offered and will not make or offer any payment, gift, or promise or give any advantage, whether directly or through intermediaries, to or for the use of any person (other than a Public Official) insofar as such payment, gift, promise or advantage would be for purposes of inducing such person to do or omit to do any act in violation of their lawful duty or to secure any improper advantage, or otherwise to do or refrain from doing something that would violate the laws applicable to the activities under the Contract.

2.4 Supplier shall cause Supplier's Personnel and Subcontractors to comply with the obligations set forth in this Appendix and to warrant the same under the terms of their agreements with any Subcontractors. In particular, Supplier shall perform compliance due diligences on all major Subcontractors in order to ensure that they shall act in strict compliance with the anti-corruption laws applicable, conducting appropriate investigations. Customer reserves the right to request proof of and/or documentation relating to such due diligences.

2.5 All financial settlements, billings and reports rendered to Customer shall accurately and in reasonable detail reflect all activities and transactions undertaken in the performance of the Contract. Supplier also shall maintain adequate internal controls to ensure that all payments made

in performance of the Contract are authorized and in compliance with the Contract. Customer reserves the right to perform itself or through a duly authorized representative, pursuant to Clause 8, audits at Supplier's premises of all payments made by or on behalf of Supplier for Goods provided and Services performed under the Contract. Supplier shall cooperate fully in any such audit, including by making the relevant books and records available to Customer or its duly authorized representative and by answering any relevant questions that Customer may have relating to Supplier's performance under the Contract.

2.6 All payments by Customer to Supplier shall be made in accordance with the terms of payment specified in Clause 9 of the Contract. The payment indications notified by the Supplier, which TotalEnergies requires to be supported by a typical type of bank certificate or adequate letter of comfort by the bank shall be deemed to constitute a representation and warranty by Supplier that the bank account so notified is owned solely by Supplier and that no person other than Supplier has any ownership of or interest in such account.

2.7 Supplier represents and warrants that no Public Official or Close Family Member of a Public Official owns or possesses, directly or indirectly, shares or any other beneficial interest in Supplier (other than through ownership of publicly traded securities that is not sufficient to constitute a controlling interest), or is a director, officer or agent of Supplier, except for any ownership, interest or position that Supplier has disclosed to Customer in writing. The foregoing representation and warranty will continue so long as the Contract remains in effect. Supplier shall notify Customer promptly and in writing of any developments that would or might affect the accuracy of the foregoing representation or warranty. In any case, if a Public Official or Close Family Member of a Public Official owns or acquires, directly or indirectly, shares or any other beneficial interest in Supplier, or is or becomes a director, officer or agent of Supplier, Supplier shall take appropriate steps to ensure that such Public Official or Close Family Member of a Public Official avoids any conflict of interest, complies with the legislation applicable in accordance with the place of performance of the Contract prohibiting conflicts of interest on the part of Public Officials and complies with the anti-corruption provisions described in this Appendix.

2.8 Notwithstanding the above, the Parties accept and acknowledge that, in the event any Supplier or Subcontractor is owned in part by a State owned company or may, whether now or in the future, be considered as a governmental entity or quasi-governmental entity at law, it is possible that a Public Official may serve as a director, officer or employee of such Supplier or Subcontractor or its subsidiaries. In such event, the Parties agree that Supplier or such Subcontractor may have one or more directors, officers or employees who qualify as Public Officials, provided that:

(a) the Public Official is occupying such position within Supplier or Subcontractor fully in accordance with laws that are attributable to such Party and as may be required there-under;

(b) the Public Official's appointment as a director, officer or employee of Supplier or Subcontractor is reviewed and approved by the State owned company;

(c) any payment to or on behalf of the Public Official is reviewed and approved by the State owned company and does not exceed the remuneration that would be reasonable for a person serving in that particular position within Supplier or Subcontractor; and

(d) such remuneration is fully consistent with Applicable Laws and the matters that are the subject of the Contract and is not made to influence any official act, decision or

omission of such Public Official or reward the Public Official in respect of any of the same that may have been taken in the past.

2.9 Without prejudice to any other rights or remedies, Customer otherwise may have hereunder or at law, including but not limited to damages for breach of the Contract, if any of the undertakings or requirements of this Appendix have not been complied with or fulfilled by Supplier in any material respect, Customer shall have the right:

(a) to suspend payment and/or require reimbursement of any advance payment made under the Contract, and/or

(b) to suspend and/or terminate the Contract for Supplier's default with immediate effect pursuant to Clause 14.

APPENDIX 1.3 – FUNDAMENTAL PRINCIPLES OF PURCHASING (FPP)

TotalEnergies integrates all aspects of sustainability at the heart of its strategy, projects and operations, and aims to be a reference with regard to commitments to the Sustainable Development Goals (SDG). Our Fundamental Principles of Purchasing, derived from our Code of Conduct, are the cornerstone of the long-term relationship we intend to forge with our suppliers. We therefore require all suppliers of Goods and services to comply with these principles and ensure compliance by their own suppliers in turn.

Suppliers are required to comply with and to ensure their own suppliers and subcontractors comply with applicable laws, as well as principles equivalent to those set forth in the Universal Declaration of Human Rights, the fundamental Conventions of the International Labour Organization, the United Nations Guiding Principles on Business and Human Rights, United Nations Global Compact, the Voluntary Principles on Security and Human Rights, and the OECD Guidelines for Multinational Enterprises. Effective policies and procedures must be implemented, in particular with respect to the principles set out below. We also expect our suppliers to continuously improve their performance on these subjects.

Principle 1: Respect human rights at work

Ensure that working conditions and remuneration of workers preserve human dignity and are consistent with the principles defined by the Universal Declaration of Human Rights and by the fundamental Conventions of the International Labour Organization.

Prohibition and prevention of child labour

- Prohibit employment of workers under the age of 18 for hazardous and night work and prohibit employment of workers under the age of 15, except where local law provides for greater protection for the child.

Prohibition and prevention of forced labour

- Ensure that no worker is coerced to work against her/his will through the use of violence, intimidation, financial coercion or threat of penalty or sanction.
- Prohibit confiscation of workers' identity documents, provided that where local law requires such document to be retained, workers must have immediate and automatic access to such documents.
- Ensure that no recruitment fees are charged to the worker.

Working conditions, remuneration and compensation

- Establish an employment contract.
- Provide a living wage and ensure compliance with a maximum number of working hours, adequate rest time and parental leave.
- Document compliance with such requirements.

Health and Safety at work

- Provide a healthy and safe workplace where workers are protected from accidents, injuries, and work-caused illness.
- When accommodation is provided by the employer, ensure that it is safe, clean and adequate as a living space.

Prohibition and prevention of discrimination and harassment at the workplace

- Prohibit harassment and practices resulting in discriminatory treatment of workers with particular attention to recruitment, compensation, benefits, or termination.

Freedom of speech, association and collective bargaining, freedom of thought, conscience, and religion

- Allow workers to choose whether to be member of a collective bargaining organization. In countries where such right is restricted, ensure employees have the right to participate in a dialogue about their collective work situation.

Grievances and Concerns

- Ensure workers can express grievances and concerns without fear of reprisal.

Principle 2: Protect health, safety, and security

Put in place an appropriate health, safety and security management system:

- Perform risk analysis and implement appropriate means and action plans to prevent those risks.
- Establish a system for monitoring events that occurred in these areas.
- Implement incident response plans and means of intervention designed to face different types of events the supplier may encounter.
- Carry out a periodic review of the relevant policies and measures and institute suitable control measures.

Principle 3: Act in favor of climate

- Implement an energy efficiency management system.
- Continuously seek to reduce greenhouses gas emissions from operations, products, and services.

Principle 4: Preserve the environment

Protection of the environment

- Limit the impact of industrial activities on the environment, including possible impacts on air quality, water resources and soils.

- Implement a systematic approach to define measurable environmental objectives, achieve them, and demonstrate that they have been achieved.
- Implement an appropriate environment risk management system based on the Avoid-Reduce-Compensate mitigation hierarchy in order to identify and control the environmental impact of activities, products or services.
- More generally, undertake the improvements needed for protecting the environment.

Promotion of circular economy and responsible use of natural resources

- Ensure that natural resources (water, soil, forests…) are used efficiently.
- Continuously seek to minimize waste production.
- Apply the "reduce, reuse, recycle, valorize" principles.

Protection of biodiversity

- Ensure that no production Site possibly having detrimental impact on the environment is located in natural protected areas listed as categories I to IV by the International Union for Conservation of Nature, in wetlands designated under the Ramsar International Convention or in Sites inscribed on the inventory of the World Heritage Natural Sites of UNESCO.
- Continuously seek to minimize biodiversity impact of operations, products and services applying the Avoid-Reduce-Compensate mitigation hierarchy.

Principle 5: Prevent corruption, conflict of interests, and fight against fraud

- Prevent and ban any form of corruption: active or passive, private or public, direct or indirect.
- Fight against fraud.
- Avoid conflicts of interest, in particular, when personal interests may influence professional interests.

Principle 6: Respect competition law

- Comply with the applicable competition law.

Principle 7: Promote economic and social development

- Create a climate of trust with stakeholders, engaging in a dialogue with local communities.
- Promote local sustainable development initiatives.
- Give local companies the opportunity to develop their business.

Compliance with these laws and principles may be audited.

Suppliers are required to cooperate with the audit process.

APPENDIX 1.4 – HYGIENE, SAFETY, AND THE ENVIRONMENT UNDERTAKINGS

1 Definitions

Commencement Date means the date when Supplier is requested to be ready to perform its obligations under the Contract.

Environment: soil, subsoil, water, air, species and their habitats and interactions.

HSE: hygiene, safety and the environment.

HSE Event : an HSE Incident, a Near-Miss or an abnormal situation or action including those that deviate from a standard, specification, procedure or rule.

HSE Incident : any sudden event on a given date which causes injury, illness or death, damage to assets or property, loss of production, or harm to the Environment or to Customer or any of its Affiliates' corporate image.

HSE Management System means one of the components of the global management system of a Party contributing to the management of the HSE risks involved in any of its activity related to the Contract or the performance of its obligations under the Contract. It includes the organisational structure, the planning activities, the responsibilities, practices, procedures, processes and resources (i.e. property and equipment and Personnel) for establishing, implementing, reviewing and maintaining the HSE policy and continuously improving the HSE performances.

Near-Miss : any event not constituting an HSE Incident but which, in slightly different circumstances, might have generated identical consequences to those of an HSE Incident.

Resources means tools, devices or machinery necessary to perform Supplier's obligations under the Contract.

2 General

2.1 Customer places and requires Supplier to place the highest importance and priority on HSE matters at all levels of its organization during the performance of the Contract.

2.2 In performing its obligations under the Contract, Supplier shall at its own cost, and shall cause its Subcontractors to, take all the appropriate precautions and measures to (i) safeguard the health of the people that may be affected by the performance of the Contract, (ii) ensure high safety levels in performing the Contract, (iii) avoid or mitigate negative impacts on the environment and (iv) protect Customer's property, equipment and Personnel at the Site.

3 HSE Compliance

3.1 In performing its obligations under the Contract, Supplier shall comply, and shall cause its Subcontractors to comply, with:

(a) All Applicable Laws relating to HSE matters;

(b) The HSE standards that would be expected in accordance with Good Industry Practice;

(c) Customer's Golden Rules for safety at work;

(d) The rules, regulations and operating procedures prevailing on the Site with respect to HSE matters and Site access conditions;

(e) Any process and procedures relating to simultaneous operations and work permits on the Site;

(f) HSE plans, work authorizations and other associated permits (including hot work permit, confined space entry permit, digging permit);

(g) Any specific requirements set out in this Appendix "Hygiene, Safety and the Environment".

3.2 Supplier shall take into account any additional opportunities to reduce risks in terms of HSE.

4 Supplier's Corporate HSE Policy and HSE Management System

4.1 Supplier shall maintain and implement a corporate HSE policy consistent with Good Industry Practice in HSE matters and with Customer's HSE policy.

4.2 Supplier shall maintain and implement a HSE Management System consistent with its Corporate HSE Policy and with Customer's HSE management system, including all relevant procedures to ensure:

(a) prevention and mitigation of HSE risks;

(b) compliance with the provisions of Article 3 of this Appendix;

(c) monitoring, and reporting to Customer, of the implementation of the requirements of this Appendix "Hygiene, Safety and the Environment", and monitoring progress against HSE objectives pre-established by Supplier;

(d) the qualification and the ability of Supplier's Personnel to carry out the required tasks and the correct maintenance and adaptedness of processes, tools, materials and the equipment to the HSE risks associated with the performance of the Contract.

4.3 Supplier shall give evidence of its Corporate HSE Policy and HSE Management System and their implementation upon request of Customer. Where the HSE Management System has been certified, information to be provided with respect to such certification shall include level and duration of certification. Any modification relating to such certification shall be communicated without delay to Customer.

4.4 Data on Supplier's HSE performance at the Site may be used freely by Customer for regular internal and/or external reporting or publication.

5 HSE Plan

5.1 Before the Commencement Date, Supplier shall:

(a) perform a Site visit and survey to assess the HSE conditions;

(b) perform a HSE risk analysis, using adequate analysis methods, and covering all HSE risks likely to result from the performance of the Contract. Such HSE risk analysis shall fully take into account any information made available by Customer concerning local specificities impacting HSE;

(c) on the basis of the above, establish a HSE Plan consistent with the provisions of this Appendix, and setting out the HSE requirements (namely all the appropriate precautions and measures to prevent and mitigate HSE risks) relevant to the specificities of the Contract, taking into account all Supplier's procedures necessary for the proper performance of the Contract.

5.2 The HSE Plan shall be drawn up and communicated to Customer before the Commencement Date.

5.3 Any modification to the HSE Plan during the course of the Contract shall be communicated to Customer before starting the concerned work.

5.4 Supplier shall be responsible for performing its obligations under the Contract in compliance with the HSE Plan.

6 Supplier HSE Organisation

6.1 Supplier shall give evidence to Customer upon its request that it has an organization and all the necessary resources to adequately implement Supplier HSE Plan.

6.2 Supplier shall ensure that Supplier's Personnel are aware of and committed to its Corporate HSE Policy, its HSE Management System, the HSE Plan and the task risk assessments required under Article 7 of this Appendix.

6.3 Supplier shall appoint a HSE representative responsible for (i) supervising and monitoring the implementation of Supplier HSE Plan and the HSE rules in force at the Site and (ii) communicating with Customer. Supplier shall inform Customer of the contact details of such HSE representative.

6.4 Supplier shall be responsible for ensuring at its own cost the safety of all Personnel involved in the performance of the Contract. This shall include, inter alia, the providing of appropriate personal protective equipment.

6.5 Supplier shall demonstrate to Customer upon its request evidence of a safety information handover system for shifts and crew change and shall be responsible for its implementation.

6.6 Supplier shall set up a medical fitness control policy and shall be responsible for its implementation. Supplier shall, and shall cause its Subcontractors to, perform all relevant and timely assessments to ensure that Supplier's Personnel involved in the performance of its obligations under the Contract are medically fit for the job they are assigned to.

6.7 The medical fitness files of Supplier's Personnel must be available for presentation at all times to all competent authorities in the course of the performance of the Contract.

6.8 The language used in managing all HSE issues shall be appropriate to ensure proper communication among Supplier's Personnel and with Customer's Personnel.

7 Work permit process

7.1 Supplier undertakes to comply with the work permit process applicable on the Site.

7.2 Within this framework, Supplier shall in particular:

(a) Provide Supplier's Personnel with initial training on the work permit process and keep their skills maintained over time;

(b) Ensure that the hazards related to the tasks have been formally identified, and that the associated risks have been analysed and assessed;

(c) Not start performing any of its obligations under the Contract without holding a duly validated work permit wherever such permit is required;

(d) Promptly stop the intervention and inform Customer in the event of discrepancy between the conditions set out in the work permit and the actual conditions of the intervention.

8 Communication with Customer

8.1 Supplier shall set up and implement a HSE monitoring and reporting system for Customer's benefit. Such system shall, inter alia, allow the reporting to Customer of any HSE Event as provided at Article 14 of this Appendix and of any risk likely to modify the HSE risk analysis provided at Article 5 of this Appendix.

8.2 Where relevant, prior to the commencement of performance of the obligations under the Contract, Customer and Supplier shall cooperate in implementing HSE measures with the aim of preventing HSE risks related to simultaneous operations.

8.3 Supplier shall actively participate in any HSE meetings organised by Customer at kick-off and/or during the course of the Contract.

9 Hazardous substances and materials, waste

9.1 All procedures involving the handling, storage, use or disposal of hazardous substances or materials, as defined by the Applicable Laws, for the performance of the Contract shall be addressed in the HSE Plan.

9.2 Supplier shall also take into account any list of hazardous substances and materials present on the Site, made available by Customer, as well as any assessment of the related HSE risks.

9.3 Customer reserves the right to deny Supplier the right to use certain hazardous substances or materials at the Site.

9.4 Supplier shall ensure that the safety data sheets and any other hazard information corresponding to any hazardous substances and materials used in the performance of the Contract shall be at all times available at Site to Customer.

9.5 Supplier shall set up an efficient waste management system complying with the Applicable Laws and with any specifications provided by Customer.

10 Environment

10.1 Supplier shall identify and evaluate all potential impacts on the Environment related to the performance of the Contract and shall implement all appropriate measures to prevent and/or mitigate these impacts. These measures shall be included in the HSE Plan.

11 Subcontractors

11.1 Supplier shall select its Subcontractors through an appropriate HSE qualification process having due regard to their HSE performance, their ability to implement an HSE policy consistent with Supplier's Corporate HSE Policy.

11.2 Supplier shall cause its Subcontractors to maintain and implement a HSE management system that is compatible with that of Supplier.

11.3 Supplier shall ensure that its Subcontractors are capable of complying with requirements identical to those set out in this Appendix.

11.4 Supplier shall set up and implement a system allowing it to monitor the HSE performance of its Subcontractors as well as their compliance with requirements identical to those set out by the provisions of this Appendix.

11.5 Supplier shall ensure that the HSE roles and responsibilities between Supplier and the Subcontractors are clearly defined.

12 Competency and Training

12.1 Supplier shall inform Customer of the presence of any new Personnel, namely Personnel having less than six (6) months experience in the relevant type of activities or less than six (6) months presence on the Site and shall provide such new Personnel with an appropriate HSE support plan.

12.2 Supplier shall ensure that the HSE awareness of Supplier's Personnel is continuously maintained and enhanced through an appropriate training plan.

12.3 Supplier shall ensure that Supplier's Personnel attend any HSE induction program requested by Customer.

12.4 Before the start of the Contract, Supplier shall inform Supplier's Personnel assigned to perform its obligations under the Contract of the risks and measures implemented.

12.5 Supplier shall ensure that Supplier's Personnel hold at all times the certificates of proficiency necessary or useful to perform the obligations under the Contract.

12.6 Upon request by Customer, Supplier shall demonstrate that Supplier's Personnel have been provided a HSE training relevant for the performance of the obligations under the Contract at the Site, including a test on Customer's Golden Rules for safety at work. The content of the HSE training and certificates shall be made available to Customer upon request.

13 Emergency preparedness

13.1 Upon request by Customer, Supplier shall communicate to Customer an emergency response procedure and have due regard to any comment by Customer.

13.2 Supplier shall ensure that Supplier's Personnel on the Site participate in any Site emergency drill organized by Customer and in programmed safety exercises.

14 HSE Event management

14.1 Supplier shall without delay report to Customer any HSE Event on the Site or occurring during the performance of the Contract, taking into account the actual or potential severity of the HSE Event.

14.2 Upon the occurrence of an HSE Event, Supplier shall:

(a) take without delay all the necessary corrective and preventive measures to mitigate the effects of the HSE Event and prevent any new HSE Event, including if necessary by initiating modification of the HSE Supplier Plan;

(b) provide Customer with all relevant information related to the HSE Event and assist Customer in the gathering of evidence and analysis of the causes of the HSE Event;

(c) take full account of the findings of the analysis of the causes within its HSE Management System and the HSE Plan.

14.3 Any member of Supplier's Personnel who believes that a task, whether or not a part of Supplier's obligations under the Contract, is unsafe or could lead to an HSE Event, shall be entitled, with no personal repercussion, to request the suspension of such task until resolution of the concern.

14.4 Without prejudice to the provisions of Article 17 of this Appendix, Customer reserves the right to direct any emergency response measures.

14.5 In case of an illness or bodily injury or search and rescue operations involving Supplier's Personnel, Customer will endeavour to provide assistance to Supplier's Personnel. Supplier shall defend, indemnify and hold harmless Customer and any of its Affiliates from any claim arising out of or in

connection with Customer or any of its Affiliates providing, failing or inability to provide such assistance and/or the performance of such operations.

14.6 The costs of such assistance provided by Customer to Supplier's Personnel shall be borne by Supplier.

15 HSE Audits

15.1 Supplier shall include in the HSE Plan and perform periodical inspections and internal HSE audits of Supplier's Personnel and Supplier's Resource during the performance of the Contract at the Site. The observations made during these audits must be communicated to Customer and translated into a regularly reviewed action plan.

15.2 Supplier shall regularly audit the performance of its HSE Management System and its implementation.

Audits may be conducted by Customer under Clause 8 on any HSE aspect of the performance of the obligations under the Contract.

15.3 Supplier shall conduct regular safety observations, covering all of Supplier's Personnel involved in the performance of its obligations under the Contract. The results of its observations must be communicated to Customer.

16 Site clean-up

16.1 Upon completing all or part of the obligations under the Contract on the Site, Supplier shall remove, at its own expense and responsibility:

(a) all Supplier's Resource;

(b) temporary installations;

(c) any wreck, debris and generally any waste; and,

(d) unless otherwise agreed, any surplus of materials.

16.2 Supplier shall clean up and, where relevant, restore and rehabilitate the Site in compliance with this Appendix.

16.3 If Supplier fails to satisfy the above requirements, Customer, following prior notification to Supplier, shall have the right to perform (or have performed) removal, clean-up, restoration and rehabilitation operations at Supplier's cost and expense, at any time.

17 Consequences of non-compliance

17.1 Without prejudice to any other provision of the Contract, in the event of non-compliance by Supplier with any of the provisions of this Appendix, Customer:

(a) may promptly notify Supplier that Customer is or will take, at Supplier's expense, all appropriate measures to correct such non-compliance should Supplier fail to meet its obligations without delay or within the time set out by Customer;

(b) reserves the right to deny access to, or the continued presence of, Supplier or any member of Supplier's Personnel on the Site;

(c) may suspend the performance of any or all parts of its obligations under the Contract in accordance with the provisions of the Contract;

(d) may terminate the Contract in accordance with the provisions of Clause 14 of the GT.

17.2 In the event of a fatality on the Site, Customer may suspend the performance of any or all parts of the obligations under the Contract in accordance with the Contract.

APPENDIX 1.5 – CYBERSECURITY REQUIREMENTS

Cybersecurity Requirements

Model contract X (Insert number)

Requirements for Type 3 contracts:	**1 to 13**
Requirements for Type 2 contracts:	**1 to 24**
Requirements for Type 1 contracts:	**1 to 33**
Additional Requirements for Type 1 contracts with contract-specific resources:	**34 to 67**

NB: Plan d'Assurances Sécurité (PAS) model must be added at the end of this appendix for contract type 1. PAS model is available on Agora in French ref n°E064 and in English ref n°E065

Table of Contents

1 TERMS AND DEFINITIONS 38
2 REQUIREMENTS FOR TYPE 1, 2 AND 3 CONTRACTS 42
3 ADDITIONAL REQUIREMENTS FOR TYPE 1 AND TYPE 2 CONTRACTS 45
4 ADDITIONAL REQUIREMENTS FOR TYPE 1 CONTRACTS 48
5 ADDITIONAL REQUIREMENTS FOR TYPE 1 CONTRACTS WITH CONTRACT-SPECIFIC RESOURCES 50

PREAMBLE

These Cybersecurity requirements set the minimum and standard framework of the rules that must be respected by the Supplier and its possible subcontractors in the context of the execution of the Contract.

These rules must be specified in the Security Assurance Plan for Type 1 Contracts.

They can be specified for Type 2 or Type 3 Contracts in a Security Assurance Plan.

Cybersecurity Requirements shall not prevail over or defeat the application of (i) applicable laws and regulations relating to the Cybersecurity of Systems and data and (ii) more precise and stringent applicable rules relating to the Cybersecurity of Systems and Data, such as certifications to standards such as ISO, ETSI or European Cybersecurity applicable to the Supplier, its products, procedures and/or services, the Internal Rules and the rules otherwise agreed by the Parties.

It is recalled that certain Information Systems and their Resources, due to their sensitivity, may be subject to regulations, in particular in terms of confidentiality (e.g. defence secrecy), technical, human and organizational obligations, control and Audit, qualification and accreditation, alert and crisis management, etc. Specific Internal Rules (including the Information Systems Security Policy) as well as specific contractual rules will also apply and prevail over these Cybersecurity Requirements.

Regarding AI Technologies, additional mandatory procedures and provisions will apply when these technologies are intended to be used within critical infrastructures (notably within the meaning of Directive (EU) 2022/2557) or sensitive or vital systems and networks of the Company, or those subject to specific Cybersecurity regulations. The same will apply to all high-risk AI systems (within the meaning of the AI Act). The stipulations in these AI requirements cannot replace or apply by default to such cases.

References to the Supplier must be understood as including the Supplier and its subcontractors, the Supplier's obligations extending to the Information Systems and Resources of its subcontractors.

Terms and definitions

The terms defined below apply only to security requirements – they may in no way be used or used as a reference in the other contractual documents of the Contract.

AI Technology: Any artificial intelligence model or system incorporated, used, and/or operated under the Contract and falling within the scope of Regulation (EU) 2024/1689 of June 13, 2024 (hereinafter "AI Act").

Audit: Set of checks to ensure the compliance of the Supplier, its services or goods, with its legal and contractual obligations in terms of Cybersecurity.

Types of Audits: organizational, compliance, configuration, and technical (intrusion, code review ...)

Authentication: A method of verifying the identity of a user accessing the Information System.

CERT (Computer Emergency Response Team) TotalEnergies: Entity (Computer Emergency Response Team) responsible for coordinating the response to IT and Cybersecurity incidents and assessing the Cybersecurity of the Company's entities and their Suppliers.

See https://totalenergies.com/cert

Classification: The classification of a Resource by the Customer provides the Supplier with a concise indication of its importance and the need for an appropriate level of protection.

Classification Profile: The classification approach, which consists in assigning a value corresponding to the potential impact of the Risks likely to affect the Resources analyzed according to the three criteria considered.

Each Resource is therefore assigned, for each of the Availability, Integrity and Confidentiality criteria, a sensitivity level (0=Low impact level to 4=High impact level)

Contract: Refers to all the documents governing the contractual relationship between the Supplier and the Customer for a defined service.

Contract-Specific Resources: Includes Resources under the responsibility of the Supplier and its subcontractors Supplier that are implemented specifically for the Contract, including in particular the workstations of the employees involved in the Contract and the Resources dedicated to the execution of the Contract Supplier.

Customer Data: Data, including personal data, to which the Supplier has access under the Contract, as well as data (including logs and metadata) generated by the Systems.

Cybersecurity: All the technical and organizational Measures necessary and proportionate to protect the Company's Information Systems and Resources, the Contract-Specific Resources, Customer Data, users and third parties that could be impacted, against events or actions likely to compromise the availability, authenticity, integrity or confidentiality of the Information Systems and Resources, as well as the Customer Data and the services they offer or make accessible.

Cybersecurity Incident: Any Event observed likely to call into question the Cybersecurity or the normal functioning of a Resource of the Information System (or a service provided by the IS function) of the Customer or a Contract-Specific Resources and likely to affect the availability, the integrity or confidentiality of the relevant Resource or Customer Data.

Enterprise Information Systems (EIS): EIS is Information Systems comprising services and applications intended for business management (office automation, human resources, customer relations, finance, treasury, purchasing, etc.).

Event: Information generated by a component of the Information System that is recorded in a log**.**

Industrial Information Systems (IIS): IIS is Information Systems comprising Systems and components that contribute directly to the production processes, integrity, safety and security of sites (command control systems, laboratory management, technical management Systems, etc.).

Information System: An organized set of Resources for processing data and providing services. The Information System is essential to the Company's activities. It includes the Enterprise Information System (EIS) and the Industrial Information System (IIS).

Internal Rules: Refers to the Customer's rules, in particular, any internal rules and procedures specific to the Information System(s) or the Customer's sites transmitted by the Customer to the Supplier or accessible from the Customer's Intranet.

Major Cybersecurity Incident: Any Cybersecurity Incident that results in temporary or permanent loss of service delivery to TotalEnergies.

Malicious Code: Any program developed for the purpose of harming or by means of a computer System or a network.

(Cybersecurity) Measure: Means to manage a Risk, which may be of an administrative, technical, managerial, or legal nature, including in particular the policy, procedures, guidelines and organizational practices or structures.

Privileged Access: Authorization to access a Resource to perform resource administration operations (e.g.

read the configuration, modify the configuration, execute a command reserved for an administrator, delete files ...).

Remediation: Implementation of security means or Measures to resolve errors, flaws, defects, or failures in Cybersecurity.

Resource (of the Information System): Includes all or part of the means, services and processes involved in the operation of the Customer Information System, such as, in particular, applications, data, technical means, equipment, networks (local, corporate, etc.). It is specified that the Resources include the means, services and processes of the Suppliers who participate in the Customer's Information System, including Cloud or SaaS service providers, service providers in charge of managed or outsourced services, etc.

(Cybersecurity) Risk: A Risk characterized by:

- a Threat or malicious action of internal or external origin on Information Systems.
- a Threat or non-malicious action, such as a failure, negligence or error of the Information Systems.

Security Committee (SECCO): Decision-making and monitoring body for action plans and Cybersecurity indicators.

Security Assurance Plan (SAP): Document describing the terms of execution of the Contract from a Cybersecurity point of view. This document describes the Cybersecurity indicators, the Cybersecurity organization and the specific Cybersecurity Measures put in place.

Security Operation Center (SOC): A Security Operations Center (SOC) is a centralized function within an organization that employs people, processes, and technologies to continuously monitor and improve the organization's security posture while preventing, detecting, analyzing, and responding to Cybersecurity Incidents.

State of Art: Principles and fundamental notions of the security of Information Systems described in particular in standards (ISO, IEC) and texts published by official bodies (ANSSI, NIST, ENISA).

Strong Authentication: Authentication based on at least 2 of the following:

- a secret known to the user only (password, PIN);
- an object owned by the user (card generating one-time passwords, smart card, USB key);
- a physical characteristic of the user (fingerprint, retinal fingerprint, hand structure, or any other biometric element).

Systems: Refers to the Information Systems of the Customer or the Supplier used in the context of the Contract.

(Cybersecurity) Threat: Potential cause of a Cybersecurity Risk, which can harm an Information System or an organization.

Vulnerability Levels: The CERT defines and specifies the levels of vulnerability (e.g. P0, P1, Standard) and which are included in the Security Assurance Plan if applicable.

Requirements for Type 1, 2 and 3 contracts

1. Raise awareness of Cybersecurity among personnel	Cybersecurity Awareness and Training
The Supplier must conduct awareness-raising actions among the personnel involved in the performance of the Contract (including subcontractors), to ensure that they are aware of the Cybersecurity rules to be applied.	

2. Manage Incidents related to Malicious Codes	Protection against malicious code
The Supplier must define and implement processes and procedures for the managing Threats and Malicious Codes. The Supplier is required to comply with its contractual and legal obligations about reporting Security Incidents to the Customer, including the breach of personal or non-personal data.	

3. Secure the mobile devices used for the Contract	Security of mobile systems, workstations, and equipment
The Supplier must ensure the existence of specific and appropriate Measures for the security of its mobile devices (all types of connected equipment) used by its personnel (and/or those of its subcontractors) in the context of the execution of the Contract.	

4. Secure the digital media used for the Contract	Security of Digital media
The Supplier must put in place Measures to protect the digital media on which the Customer Data resulting from the execution of the Contract is copied, saved and/or archived (backup). Computer media must be subject to a formalized Classification and must be in line with the type of data copied, backed up and/or archived (backup). The inventory of computer media must be available and kept up to date. Backup and computer archiving media must be secured and protected against illegal acts and environmental Risks. The transport of computer media must be subject to a documented procedure.	

5. Alert in case of a Major Security Incident	Cybersecurity Incident Management
Major Security Incidents must be reported to the CERT TotalEnergies within four (4) hours from the moment the Supplier becomes aware of them, specifying in particular the nature and extent of the Major Security Incident, proven and potential, as well as any information to enable the Customer to assess the consequences for himself. The Supplier actively collaborates with the Customer and regularly updates and completes this information.	

6. Respond to requests from a crisis unit of the Client	Cybersecurity Incident Management

The Supplier must have a crisis management organization allowing it to respond to requests from the Customer's crisis unit as soon as possible.

7. Test the continuity of business related to the Contract	Business Continuity Requirements

The Supplier must carry out systematic tests of its organizational, human, and technical solutions for ensuring business continuity and disaster recovery, at the end of their implementation or evolution, supplemented by tests and regular exercises to evaluate the functioning of all the continuity and disaster recovery plans that it has defined.

8. Favor the use of collaborative tools	Collaborative tools & shared Workspaces

In its exchanges with the Customer, the Supplier must use, as far as possible, the collaborative work tools suggested or made available to it by the Customer. In certain cases, in particular for reasons of confidentiality, the Supplier will be obliged to use the collaborative work tools of the Client.

9. Delete e-mail messages and documents related to the Contract at the end of the Contract	Collaborative tools & share Workspaces

Unless otherwise stipulated in a contractual document that takes precedence over these requirements and unless there is a mandatory legal obligation or for the purposes of certifying the product or service that is the subject of the Contract, the Supplier must delete from its own Resources, including Contract-Specific Resources, Customer Data and electronic messages and documents, within a maximum period of one month from the termination of the Contract for any reason whatsoever.

10. Comply with rules governing messaging and collaborative tools	Collaborative tools & shared Workspaces

The Supplier must comply with the rules of good practice associated with messaging and collaborative tools provided to it by the Customer.

11. Declare AI Technologies Used in the Contract	Knowledge of AI Technologies

The Supplier must declare in writing to the Client, before any use, the AI Technologies they wish to use under the Contract, from its signing and at any time during its execution. The same applies in case of any modification of the AI Technologies during the execution of the Contract.

The Client may oppose in writing the use of AI Technologies, without having to justify and without compensation or indemnification to the Supplier, with the Contract continuing under the initially agreed conditions until its term.

The AI Technologies authorized on the day of the signing of the Contract are exhaustively specified in the Annex Description of Services.

12. Compliance of AI Technologies Used in the Contract	Compliance of AI Technologies

The Supplier guarantees for itself and its subcontractors that the AI Technologies:

- Do not include any prohibited AI (within the meaning of the AI Act) and that no prohibited AI has been previously used in relation to the AI Technologies in the execution of the Contract;
- Do not include high-risk AI, except with the prior written consent of the Client and subject to the application of specific and prior procedures, contractual and technical conditions provided for by the AI Act;
- Comply with all applicable laws, including the provisions of the AI Act, and are updated according to changes in applicable laws, within legal deadlines, at no additional cost to the Client;
- Have not been subject, in the last six (6) months, to interruptions resulting from the use of any emergency mechanism to prevent the AI technologies from executing or performing a particular function;
- Are implemented within the framework of strict specifications, design, and control and supervision protocols to restrict access to its AI Technologies and training, testing, verification, and improvement data, and that there has been no unauthorized access to the algorithm or software incorporating the AI Technologies or to the training, testing, verification data used to train and/or improve the AI Technologies

13. Monitor Operations Performed on AI Technologies	Compliance with Obligations on AI Technologies

The Supplier:

- Provides the Client with all technical and functional documentation regarding the AI Technologies.
- Implements all obligations defined in the AI Act, particularly quality assurance measures, risk management, human oversight, information, and transparency.
- Keeps information in a readable and easily accessible form for the Client or regulatory authorities, explaining the operations carried out, the results produced, and the decisions made or facilitated by the AI Technologies.

Additional requirements for Type 1 and Type 2 contracts

14. Appoint a security officer	Cybersecurity Governance
The Supplier must designate a security officer. This security officer is the single point of contact for security throughout the duration of the Contract. It must be easily reachable by the Customer, in a secure manner and the means of communication must be established at the start of the Contract.	

15. Appoint a Remediation officer	Cybersecurity Governance
The Supplier must designate, within its teams, a person responsible for the application of the Remediation, in relation to the Customer.	

16. Produce qualification evidence	Supplier's Cybersecurity Certifications
The Supplier must produce any certification / accreditation / label / reference to the Customer supporting its competence, in particular in the Cybersecurity's domain as well as that of its employees and subcontractors within the scope of the Contract. Evidence of defined qualification imposed within a specific regulatory framework must also be made available.	

17. Maintaining Cybersecurity Qualifications	Supplier's Cybersecurity Certifications
The Supplier is responsible for maintaining the required certifications, accreditations and labels. Cybersecurity certifications required under the Contract must be valid for at least the duration of the Contract.	

18. Notify in case of any loss of qualification	Supplier's Cybersecurity Certifications
The Supplier must notify the Customer as soon as possible, and at the latest within seven (7) working days, in the event of loss of accreditation, label or certification, whether a "Company" certification or one or more required certifications applying to the personnel, equipment, services or processes of the Supplier or that of its subcontractors.	

19. Train personnel on Cybersecurity issues	Cybersecurity Awareness and Training
The Supplier must ensure that the employees assigned to the performance of the Contract (including subcontractors' stakeholders) acquire the knowledge and skills required for the performance of the tasks entrusted to them and the issues related to Cybersecurity. The Supplier must undertake the necessary training actions to maintain the skills of all employees and stakeholders concerned. The Supplier must, on request, provide evidence of the existence of an awareness and training program.	

20. Secure the workstations used under the Contract	Security of mobile systems, workstations, and equipment
The Supplier must ensure the hardening of the workstations used by its personnel (and/or subcontractors) in the context of the performance of the Contract so that this equipment does not constitute a vector of breach of the security of the Resources used for the performance of the Contract (e.g. theft of equipment resulting in the disclosure of confidential information or the loss of essential data, the propagation of Malicious Code or the logical intrusion and illicit access to sensitive Resources).	

21. Validate the Cybersecurity Measures implemented	Design – implementation – evolution of Contract-Specific Resources
The Supplier must proceed, prior delivery, to the technical verification of the Cybersecurity Measures implemented and return these results to the Customer at the end of each control campaign. Where applicable, this report will mention the deviations from the previously validated security specifications and the identified residual security Risks.	

22. Implement a Cybersecurity Incident Management Process	Cybersecurity Incident Management
The Supplier must put in place the technical, human, and organizational means to detect, alert, support and remedy Cybersecurity alerts or Incidents, and in particular to report to the Customer Cybersecurity Incidents concerning the Contract-Specific Resources or the Customer Data used under the Contract, to react effectively according to the nature and severity of the Incidents detected, to limit their impacts and to resolve quickly and formally all Cybersecurity Incidents.	

23. **Protect the Customer' data used in the context of the Contract**	**Collaborative tools & shared spaces**

The Supplier must ensure that all data and documents relating to the Customer (including Customer Data or those generated by the service defined in the Contract or inventory data) remain on the dedicated and secure environments.

The transfer of data or documents outside these environments is strictly prohibited. In particular, the documents and messages exchanged under the Contract must not be communicated to third parties without the prior consent of the Customer.

The Supplier must encrypt electronic messages – regarding Customer Data – exchanged with the Customer at the State of the Art.

24. **Comply with best practices in secure development**	**Design – implementation – evolution**

The programs and applications developed by the Supplier under the Contract must comply with the State of The Art, in terms of security of computer developments and in particular the recommendations of ENISA, ANSSI and OWASP (Open Web Application Security Project). These best practices are described in the Security Assurance Plan and are validated by the Security Committee.

The Provider will also apply the principles of "security by design", "security by default", considering, where appropriate, the specificities imposed by the processing of personal data.

The Customer may provide a specific requirements document on Cybersecurity according to the technologies implemented.

Additional requirements for Type 1 contracts

25. **Define Cybersecurity roles and responsibilities**	**Cybersecurity Governance**

The Supplier must implement Cybersecurity governance to guarantee the level of security expected by the Customer and to meet all Cybersecurity requirements, general and specific, provided for in the Contract and all its Appendix. In the event of subcontracting, the Supplier must establish its own governance with its subcontractors.

This Governance is based in particular on the Supplier's participation in the Security Committee (SECCO) to meet according to the terms defined by the parties in a Security Assurance Plan (SAP).

The topics of the Security Committee will focus on the achievement of the security levels expected of the Customer, the Security Incidents that have occurred, any security derogations impacting the Customer, ongoing Security Incidents, the results of Audits or certifications conducted.

Action plans resulting from Risk analyses or Cybersecurity Audits must be reviewed during the Security Committees.

The processes of Remediation, detection and reaction must be validated by the Security Committee.

26. **Provide reporting on Remediation actions within the scope of the Contract**	**Remediation Management**

The Supplier must draw up and provide, according to the terms and frequency defined in the Security Assurance Plan, the reports defined by the Security Committee.

27. Hold administrators accountable	**Administration of Resources**

The Supplier must ensure that its personnel (and those of its subcontractors) assigned to administrators' functions are held accountable for its actions carried inherent in the privileges granted.

The process of hold administrators accountable of their actions must be formalized (documented) and traceable.

28. Ensure that administrator workstations always remain secure	**Administrator Workstation Management**

The Supplier must ensure that the workstations used for administration are maintained in a safe condition throughout the duration of the Contract, and in particular kept up to date and free of viruses or Malicious Code in order not to represent a Threat to the Company Information System.

29. Restrict Internet access from administrator's workstations	**Administrator Workstation Management**

The accounts of administrators and workstations used for administration must be configured to limit access to the Internet (e-mail, browsing) to the strict needs necessary for the performance of the Contract.

30. Apply the principle of least privilege for administrators	**Administrator Workstation Management**
Supplier's employees (and those of its subcontractors) with administrator rights must have personal and unique accounts (no shared accounts) and respect the separation of roles for administrator actions. Administrator rights must be assigned and managed in accordance with the principle of least privilege.	

31. Encrypt administrator workstation data	**Administrator Workstation Management**
All storage media used for the administration of the Customer Information System must be encrypted. Administrator sessions must be automatically interrupted after a specified period of inactivity and in accordance with the State of The Art.	

32. Ensure the physical security of administrator workstations	**Administrator Workstation Management**
The Supplier must ensure that it implements anti-theft devices and the prevention of visual indiscretions. Administrator operations must under no circumstances be carried out in a space open to the public or visible to the public.	

33. Provide reporting on Cybersecurity Incidents	**Cybersecurity Incident Management**
The Supplier must reports relating to CyberSecurity Incidents up to date and submit them to the Customer according to the periodicity and with the information provided for in the Security Assurance Plan.	

Additional requirements for Type 1 contracts with Contract-Specific Resources

The following requirements apply only if the Contract includes resources (equipment) under the responsibility of the Supplier and its subcontractors that are implemented specifically for the Contract, including in particular the workstations of the employees involved in the Contract and the Resources dedicated to the execution of the Contract.

34. **Map Contract-Specific Resources**	**Knowledge of Resources**
Supplier must map the Contract-Specific Resources implemented under the Contract in the form of architectural schematics and must maintain an inventory detailing the main features necessary to maintain security. This mapping must be validated by the Security Committee.	

35. **Maintain Contract-Specific resource mapping up to date**	**Knowledge of Resources**
The Supplier must maintain the mapping of the Contract-Specific Resources up to date. Major changes must be presented to the Security Committee within a sufficient and reasonable time before being implemented.	

36. **Classify Contract-Specific Resources**	**Knowledge of Resources**
The Supplier must identify the various Contract-Specific Resources and establish, in collaboration with the Customer and based on the Customer's reference system, a Classification of these Resources.	

37. **Train actors on the classification of Contract-Specific Resources**	**Knowledge of Resources**
The Supplier must train any actor involved in the use or management of the Contract-Specific Resources on the Classification Profile of these Resources. Administrators must master with the applicable Cybersecurity Measures.	

38. Analyze Cybersecurity Risks on Contract-Specific Resources	**Cybersecurity Risk Management**
The Supplier must carry out and keep up-to-date Cybersecurity Risk Analysis of the Contract-Specific Resources, including the data processed by these Resources, according to a mutually agreed method of analysis. The Supplier must be able to provide at any times a detailed report on all the Risks identified, classified by sensitivity, the means of prevention or mitigation and to reveal the residual Risks.	

39. **Apply an action plan to reduce the identified Risks**	**Cybersecurity Risk Management**
The Supplier must put in place, at its own expense, an action plan in connection with the analysis of Cybersecurity Risks, or the results of a Cybersecurity Audit, to reduce or prevent the occurrence of these Cybersecurity Risks or to limit their consequences. The Supplier must implement the necessary remediation measures following the notifications by the Customer as part of its data leakage program.	

40. **Protect Contract-Specific Resources against Malicious Code**	**Protection against malicious code**
The Supplier must put in place, for its Contract-Specific Resources, a protection device against the Malicious Codes.	

41. **Provide a periodic status report on efforts to combat Malicious code**	**Protection against Malicious Code**
The Supplier must regularly present to the Security Committee a quantitative (completeness) and qualitative (effectiveness) monitoring report of the means of combating Malicious Code deployed to protect the Contract-Specific Resources, according to a periodicity to be defined at the time of the firs Security Committee.	

42. **Harden the system base of Contract-Specific Resources**	**Security of system bases, workstations, and mobile equipment**
The Supplier must implement the necessary and relevant technical, human, and organizational Measures, to ensure the security of the base Systems (operating Systems, middleware, applications and related communication and security services) of the Contract-Specific Resources. These Measures must make it possible to preserve the confidentiality, availability and integrity of the data processed.	

43. Protect Contract-Specific Resources data	**Data protection Security of system bases, workstations, and mobile equipment**
The Supplier must document and implement the necessary and relevant means to secure the administration, maintenance, and operation of the System bases (operating Systems, middleware, applications and related communication and security services) of the Contract-Specific Resources.	

44. **Protect network used by the Contract-Specific Resources**	**Network Security**
The Supplier must deploy and update the security Measures, necessary, relevant, and in accordance with the State-of-the-art, to ensure the security of the networks used by the Contract-Specific Resources, to prevent or limit the consequences of Cybersecurity Risks.	

45. **Apply an authorization procedure for access to Contract-Specific Resources**	**Logical access controls and Authorizations**
The management of logical access to Contract-Specific Resources, implemented by the Supplier for the purposes of the Contract, must be described in a Security Assurance Plan (if any) or in a document sent to the Customer before the start of the Services/Supply and each time it is updated. Access to the Customer's Information System is subject only to the Customer's rules and procedures.	

46. **Audit the Cybersecurity of Contract-Specific Resources**	**Cybersecurity Audits**
Supplier must conduct Cybersecurity Audits of Contract-Specific Resources. These Audits mainly concern compliance with the requirements set out in this document. They may also relate to the Cybersecurity Measures applicable to specific regulations, such as those applicable to the processing of personal data. These Audits do not exclude the application of other contractual provisions relating to Audits of the Supplier's Resources and Information Systems, including pen testing / red team Audits. These Audits are the responsibility of the Supplier, unless otherwise agreed in advance by the Parties.	

47. **Transmit Cybersecurity Audit results on the Contract-Specific Resources**	**Cybersecurity Audits**
The results of the Audits carried out by the Supplier on the Contract-Specific Resources will be communicated to the Customer. An Audit certificate, as well as a summary of the Audit report and the progress of the Remediation and improvement actions, will be given free of charge to the Customer no later than thirty (30) working days after the date of the Audit report. All Remediation and improvement actions will be at the expense of the Supplier.	

48. **Remedy Vulnerabilities in Contract-Specific Resources**	**Remediation Management**
The Supplier must define and implement a Remediation process to correct vulnerabilities and misconfigurations of The Contract-Specific Resources.	

49. **Coordinate Remediation within contractual deadlines**	**Remediation Management**
The Supplier must implement the necessary means to apply the Remediations on the Contract-Specific-Resources, within the deadlines defined in the Security Assurance Plan for the Vulnerability Levels "Critical" or “P0”, “Urgent” or “P1”, and Standard (default). The P0 and P1 remediations are defined by the CERT TotalEnergies and communicated to the Supplier.	

50. **Separate Production Information Systems environments from non-**	**Design – implementation – evolution of Contract-Specific**

production environments	Resources
The Supplier must ensure the separation of the environments of production Information Systems and non-production Information Systems. Production data must not be used in non-production environments without the prior written consent of the Customer.	

51. Specify Cybersecurity Measures to meet requirements for Contract-Specific Resource evolutions	Design – implementation – evolution of Contract-Specific Resources
The Supplier must specify and document the security Measures to be implemented to respond, as part of the design and/or evolution projects of the Contract-Specific Resources, the levels of security and continuity of service required by the Customer. The Supplier must alert the Customer of a possible inability to offer Cybersecurity Measures to meet the required security requirements.	

52. Protect physical access to Contract-Specific Resources	Categorization of security zones
The Supplier must ensure that the physical security Measures adapted to the level of sensitivity of the Contract-Specific Resources, including data processed under the Contract, and in accordance with applicable regulations, are in place. The Supplier must ensure the protection of physical access to the various security zones in which the Contract-Specific Resources are located by means of graduated and relevant devices depending on the type of zone to be secured. The Supplier must ensure that the monitoring and control Measures for physical access protection devices are in place.	

53. Fire protection of Contract-Specific Resources	Protection against environmental Risks
The Supplier must ensure the implementation of fire safety Measures to protect the Contract-Specific Resources. These Measures must include, in particular: - Fire detection means. - Fire suppression means. - Measures for periodic verification of the means of protection and firefighting. - Procedures to be implemented in the event of fire. The Supplier must communicate to the Customer the list of fire protection Measures put in place.	

54. Protection against water damage	Protection against environmental Risks
The Supplier must ensure the implementation of the water damage protection Measures. The Supplier must communicate to the Customer the list of water damage protection Measures put in	

place.

55. **Ensure the provision of essential services for Contract-Specific Resources**	**Protection against environmental Risks**
The Supplier must ensure the installation and proper maintenance of the electrical supply, air conditioning and protection of the Contract-Specific Resources.	

56. **Transmit events generated by a Cybersecurity Incident impacting Contract-Specific Resources**	**Traceability and monitoring**
If necessary, the Security Committee can define the feared Events and detection scenarios (logs, events or detection rules) to be transmitted to the Customer's SOC so that it is able to detect the occurrence. These events generated by Contract-Specific Resources must be addressed to the Customer's log collection systems.	

57. **Implement a Security Operations Center (SOC)**	**Traceability and monitoring**
The Supplier must monitor through a Security Operation Center (SOC) the Contract-Specific Resources that are not integrated into Customer's SOC. The Supplier must establish, at the start of the contract, a communication protocol between its SOC and that of the Customer.	

58. **Report Cybersecurity Incidents**	**Cybersecurity Incident Management**
The Supplier must notify the CERT TotalEnergies of any incident affecting or likely to affect the Cybersecurity of the Contract-Specific Resources, within the deadlines and according to the terms agreed contractually or in application of a regulation, this period being fixed in default at a maximum of twenty-four hours from the moment when the Supplier becomes aware of the Cybersecurity Incident.	

59. **Transmit Events allowing Cybersecurity monitoring of certain Contract-Specific Resources**	**Traceability and monitoring**
The Supplier must transmit to the Customer's Security Operation Center (SOC), at first request and within a time frame adapted to the situation that generated the request, all Events associated with a Cybersecurity Incident impacting the Contract-Specific Resources. These Events must be addressed to the Customer's technical means of logging.	

60. **Implement a Computer Emergency Response Team (CERT)**	**Cybersecurity Incident Management**
The Supplier must describe in the Security Assurance Plan its response organization to a Cybersecurity	

Incident, equivalent to an organization of a CERT (Computer Emergency Response Team) for the monitoring and response to Cybersecurity Incidents involving Contract-Specific Resources that are not integrated into SOC and CERT devices of TotalEnergies. It designates a contact point capable of reporting to the CERT TotalEnergies.

The Supplier must establish a communication protocol between its CERT and that of the Customer.

61. **Use the means of Authentication provided**	**Administration of Contract-Specific Resources**

The Supplier will use the means of Authentication made available by the Company to access the Customer's Information Systems.

The means of Authentication to access the Contract-Specific Resources must be previously validated by the Customer.

62. **Protect passwords for Contract-Specific Resources**	**Administration of Contract-Specific Resources**

The personnel assigned to the Contract must protect their passwords and their means of Authentication, in accordance with the methods validated by the Security Committee and alert without delay the Security Operation Center (SOC) of the Customer in case of compromise or suspicion of compromise.

63. **Secure Contract-Specific Resource administration flows**	**Administration of Contract-Specific Resources**

The Supplier must use the means and methods of access validated by the Security Committee to administer the Contract-Specific Resources.

The Supplier undertakes not to attempt to circumvent the Cybersecurity Measures put in place by the Client.

64. **Track Administrator Actions on Contract-Specific Resources**	**Administration of Contract-Specific Resources**

The Supplier must ensure that the actions of the administrative accounts used on the Contract-Specific Resources are logged, retained for a default period of twelve (12) rolling months, and that Events are Audited for suspicious activities or actions.

65. **Ensure availability of Contract-Specific Resources**	**Business Continuity Requirements**

The Supplier must assess the Risks of unavailability of the Contract-Specific Resources that could be detrimental to the Customer.

The Supplier must implement solutions (technical, human, and organizational) covering the scenarios of unavailability identified, and making it possible to ensure the minimum level of service required by the Customer in a crisis situation and the resumption of service under conditions that comply with the tolerance thresholds defined with the Customer.

66. **Emergency Backup**	**Business Continuity**
The Supplier must carry out separate production backups and backup backups covering all the Contract-Specific Resources (configuration of System, network and telecommunications equipment, basic software, applications**,** and Customer data). The Supplier must outsource the backup (used as part of the execution of continuity plans) to a location sufficiently distant from the production site not to suffer damage from a disaster that could impact it. The Supplier must ensure the ability to permanently access all emergency backups, regardless of their storage location.	

67. **Document the continuity of business related to the Contract**	**Business Continuity Requirements**
The Supplier must carry out systematic tests of its organizational, human, and technical solutions for ensuring business continuity and disaster recovery, at the end of their implementation or evolution, supplemented by tests and regular exercises to evaluate the functioning of all the continuity and disaster recovery plans that it has defined. The Supplier must obtain the Customer's written consent before conducting any tests and exercises based on a partial or complete and programmed shutdown of the Contract-Specific Resources or its other Resources necessary for the Supply (including any switch to backup systems). All testing and exercises of disaster recovery and business continuity devices must follow protocols documented by Supplier. Their execution must be the subject of a balance sheet showing the results in accordance with expectations and /or anomalies detected**,** which the Supplier must transmit to the Customer**,** and which will be commented in Security Committee meeting.	

End of document.