

CONDITIONS GENERALES POUR L'ACHAT DE SERVICES (CG)

1	DEFINITIONS ET INTERPRETATION	2
2	EXECUTION TARDIVE OU MAUVAISE EXECUTION	5
3	EQUIPEMENTS, MATERIELS, OUTILS ET BIENS	5
4	TRANSFERT DE PROPRIETE ET DES RISQUES RELATIFS AUX SERVICES	5
5	GARANTIES RELATIVES AUX SERVICES	6
6	RECEPTION DES SERVICES	6
7	OBLIGATIONS DU FOURNISSEUR	7
8	AUDIT ET COMPTABILITE	8
9	PRIX, FACTURATION ET PAIEMENTS	9
10	PROPRIETE INTELLECTUELLE	10
11	CONFIDENTIALITE	12
12	RESPONSABILITE ET INDEMNISATION	12
13	ASSURANCES	13
14	RESILIATION	14
15	FORCE MAJEURE.....	15
16	CESSION	16
17	SOUS-TRAITANCE	16
18	PRODUITS TOTALENERGIES	17
19	DISPOSITIONS DIVERSES.....	17
20	DROIT DU CONTRAT ET RESOLUTION DES LITIGES	19
21	SANCTIONS ECONOMIQUES ET CONTROLE DES EXPORTATIONS	19
	APPENDICE 1.1 – REGLES DE LUTTE CONTRE LE TRAVAIL DISSIMULE	21
	APPENDICE 1.2 – REGLES ANTI-CORRUPTION	23
	APPENDICE 1.3 – PRINCIPES FONDAMENTAUX DANS LES ACHATS (PFA)	26
	APPENDICE 1.4 – HYGIENE, SECURITE ET ENVIRONNEMENT (HSE)	29
	APPENDICE 1.5 – EXIGENCES DE CYBERSECURITE.....	36

1 DEFINITIONS ET INTERPRETATION

1.1 DEFINITIONS

Dans le Contrat, les termes suivants auront, sauf si le contexte l'exige autrement, la signification qui leur est attribuée ci-dessous :

Autorité de Sanctions désigne toute autorité compétente en matière d'adoption, d'administration, de mise en œuvre et d'exécution des Lois et Réglementations sur les Sanctions : (a) des États-Unis ; ou (b) de l'Union européenne ; ou (c) de la République française.

Bonnes Pratiques de la Profession désigne les pratiques, méthodes et procédures et le niveau de compétence, de diligence, de prudence et de prévoyance, qui sont raisonnablement attendus d'un entrepreneur professionnel, compétent et expérimenté, exerçant des activités identiques ou similaires à celles envisagées aux termes du Contrat, dans des circonstances identiques ou similaires.

Client désigne la personne physique ou morale désignée comme telle dans le Contrat concerné.

Commande désigne les documents émis par le Client pour l'exécution de Services par le Fournisseur. Les Commandes peuvent être émises par le Client par voie électronique (via SAP ou un système similaire). Si un modèle de Commande a été convenu dans le Contrat concerné, les Commandes devront être émises sous une forme similaire à celle convenue.

Conforme désigne le fait que les Services :

- (a) soient conformes (i) aux spécifications et à la description des Services aux termes du Contrat, (ii) aux Bonnes Pratiques de la Profession et (iii) à toute Loi Applicable ; et
- (b) soient (i) exempts de défauts imputables à la conception, aux matériaux ou à la fabrication, et (ii) propres à tout usage tel que prévu aux termes du Contrat.

Contrat désigne les documents contractuels convenus entre les Parties et régissant la relation contractuelle entre le Fournisseur et le Client concernant les Services, y compris, le cas échéant, les documents suivants et leurs Appendices, conformément à l'ordre de priorité tel qu'énoncé ci-dessous :

- (a) la Commande ;
- (b) le(s) contrat(s) d'application locale ; et/ou
- (c) toutes autres conditions particulières ;

qui renvoient aux présentes conditions générales (« **CG** ») et les incluent directement ou indirectement.

- (d) les présentes CG

En cas de divergence ou de contradiction entre les dispositions des documents listés ci-dessus :

- toutes modifications apportées aux CG aient été expressément convenues par écrit ;
- le corps d'un document prévale sur ses Appendices ; et
- les Règles Obligatoires prévalent sur tous les autres documents.

Contrôle désigne la détention, directe ou indirecte, de plus de cinquante (50 %) des droits de vote ou du capital social ; et un « **Changement de Contrôle** » désigne toute prise de participation, cession, fusion ou autre opération qui a pour effet de modifier, directement ou indirectement, le Contrôle de la Partie. Le verbe « **Contrôler** » et le terme « **Contrôlé** » seront interprétés en conséquence.

Date d'Effet désigne, selon le contexte, la date d'entrée en vigueur du Contrat concerné.

Données Client désigne les informations et les données, y compris à caractère personnel, auxquelles le Fournisseur et son Personnel a accès au titre du Contrat.

Éléments Associés désigne, le cas échéant, toutes fournitures, biens, accessoires, équipements, documents et données fournis par le Fournisseur dans le cadre de la fourniture de Services, à l'exception des équipements, matériels et outils mentionnés à l'Article 3 des présentes.

Force Majeure désigne la survenance effective de tout acte ou événement :

- imprévisible ;
- insurmontable ;
- en dehors du contrôle de la Partie qui s'en prévaut ; et

qui empêche cette Partie d'exécuter, totalement ou partiellement, ses obligations aux termes du Contrat.

Sous réserve que ces critères soient satisfaits, la Force Majeure inclut les événements tels que les catastrophes (épidémie, raz-de-marée, foudre, tremblement de terre, ouragan, inondation), les guerres (qu'elles soient déclarées ou non), les émeutes (autres que parmi le Personnel du Fournisseur ou le Personnel du Client), les troubles civils ou militaires, les grèves régionales ou nationales (sauf les grèves ainsi que les blocages d'établissement ou toute autre action ou litige professionnel limités à ou émanant du personnel du Fournisseur ou de ses Sous-Traitants), toutes Lois Applicables (par exception, les Lois et Réglementations sur les Sanctions promulguées après la Date d'Effet qui seront considérées comme imprévisibles) et les actes de tout tribunal, gouvernement ou autorité gouvernementale ou de tout représentant de ceux-ci.

Fournisseur désigne toute personne physique ou morale désignée comme telle dans le Contrat concerné.

Groupe du Fournisseur désigne le Fournisseur et toute Société Apparentée et tout membre de leurs Personnels respectifs ou leurs Sous-Traitants.

Liste de Sanctions désigne toute liste de personnes ou entités faisant l'objet de sanctions et dont les actifs sont gelés et administrés par l'Office of Foreign Assets Control du département du Trésor américain (listes de ressortissants ou de personnes nommément désignés), l'Union européenne (liste consolidée de personnes physiques, groupes et entités faisant l'objet de sanctions financières) ou la République française, telle qu'amendée, complétée ou remplacée le cas échéant.

Lois Applicable désigne l'ensemble des lois, ordonnances, règles, règlements, arrêtés, décrets et actes de même nature, émanant d'une autorité gouvernementale, fédérale, nationale ou locale, ou de toute autre autorité ou agence ayant compétence à l'égard des Parties, ou l'une d'entre elles, des Services, des équipements du Fournisseur ou du Site, qui sont en vigueur ou à venir, y compris les Lois et Réglementations sur les Sanctions. Les références à toute Loi Applicable doivent être interprétées comme incluant une référence à cette loi telle que modifiée, amendée, étendue, ou consolidée, que ce soit avant ou après la date du Contrat et de toute législation subordonnée adoptée en vertu de cette loi.

Lois et Réglementations sur les Sanctions désigne toutes lois, réglementations, embargos ou autres mesures restrictives applicables en matière de sanctions économiques, financières, contrôle des exportations ou sanctions commerciales, adoptés, administrés, mises en œuvre et/ou exécutés par une Autorité de Sanctions ou agence compétente.

Partie(s) désigne, relativement à un Contrat, le Client et/ou le Fournisseur, collectivement ou individuellement.

Personnel désigne les dirigeants, administrateurs, salariés, mandataires.

Personne Sanctionnée désigne toute personne physique ou morale listée, détenue (directement ou indirectement) à 50 % ou plus, ou contrôlée (si le contrôle est exercé conformément aux Lois et Réglementations sur les Sanctions), par une partie inscrite sur une Liste de Sanctions.

Règles Obligatoires désigne : (a) toutes règles et procédures internes spécifiques au(x) Site(s) transmises par le Client au Fournisseur ou à tout membre du Groupe du Fournisseur ; (b) les règles de lutte contre le travail dissimulé (telles que définies en APPENDICE APPENDICE 1.1) ; (c) les règles anti-corrupcion (telles que définies en APPENDICE APPENDICE 1.2) ; (d) les principes fondamentaux dans les achats (tels que définis en APPENDICE APPENDICE 1.3) ; (e) les règles hygiène, sécurité et environnement (telles que définies en APPENDICE APPENDICE 1.4) ; et (f) les exigences de Cybersécurité (telles que définies en APPENDICE APPENDICE 1.5).

Site désigne le(s) lieu(x), tel(s) que défini(s) dans le Contrat concerné, où les Services devront être réalisés.

Services désigne tous travaux et services qui doivent être effectués par le Fournisseur, ainsi que, le cas échéant, les Eléments Associés, tels que définis dans le Contrat.

Société Apparentée désigne, pour une entité donnée, toute autre entité juridique qui, directement ou indirectement, Contrôle ou est Contrôlée par une entité qui Contrôle une Partie.

Sous-Traitants désigne les sous-traitants du Fournisseur, qui réalisent une partie des obligations du Fournisseur aux termes du Contrat.

1.2 INTERPRETATION

- (a) A moins qu'il n'en soit expressément stipulé autrement, chaque fois que les expressions et termes suivants et leurs dérivés sont utilisés dans toute Partie du Contrat, ils devront être interprétés comme suit :
 - (i) les termes « incluant », « inclut », « tel que » et autres termes similaires seront réputés être complétés par l'expression « sans limitation » ;
 - (ii) les termes « rapport », « rendre compte », « demander », « soumettre », « émettre », « notifier », « donner instruction », « informer », « consentir », « consentement », « approuver », « approbation », « approuvé » et autres termes similaires seront réputés être complétés par l'expression « par écrit » ; et
 - (iii) les termes « biens » et « équipements » seront interprétés comme incluant les biens et équipements opérés, loués ou autrement utilisés par ou en possession de la personne concernée.
- (b) Lorsque le contexte l'exige, les termes au singulier incluent également le pluriel et vice-versa.
- (c) Les titres et sommaires sont insérés uniquement pour convenance et ne sauraient en aucun cas limiter ou influencer l'interprétation du Contrat.
- (d) Une approbation ou instruction par le Client ne pourra en aucun cas être interprétée comme libérant le Fournisseur de tout engagement, obligation ou responsabilité aux termes du Contrat ou à tout autre titre.
- (e) « Par écrit » ou « écrit » signifient toute communication faite par lettre, avis, courrier électronique ou par tout système de commande ou de facturation électronique tel que décrit au Contrat.

- (f) Les références à toute personne, y compris une Partie, comprennent les ayants droit et cessionnaires de cette personne (à moins que la cession au cessionnaire ou à l'ayant droit ait été réalisée en violation des dispositions du Contrat). Les références au Contrat ou à tout autre document constituant des références au Contrat ou à cet autre document, tel qu'ils peuvent être modifiés, novés, amendés ou remplacés à tout moment.
- (g) Chaque disposition du Contrat sera interprétée comme ayant fait l'objet d'une négociation entre les Parties et comme si toutes les Parties avaient participé de manière égale à sa rédaction. En conséquence, les Parties reconnaissent et conviennent que toute règle d'interprétation selon laquelle un document doit être interprété contre l'une des Parties sera inapplicable au Contrat.

2 EXECUTION TARDIVE OU MAUVAISE EXECUTION

- 2.1** Le respect des délais est une obligation essentielle du Contrat. Le Fournisseur doit fournir des Services Conformés dans les délais et/ou périodes définis dans le Contrat. Si le Fournisseur estime qu'il pourrait ne pas être en mesure de fournir les Services conformément à ces délais ou périodes, il doit immédiatement en informer le Client et fournir les raisons de ce retard ainsi que les mesures correctives appropriées.
- 2.2** De plus, au titre du Contrat, le Fournisseur est soumis à une obligation de résultat et garantit la fourniture dans les délais prescrits de Services Conformés.
- 2.3** Si le Fournisseur n'exécute pas les Services dans les délais et/ou périodes définis dans le Contrat ou s'il manquait à son obligation de fournir des Services Conformés, le Client aura :
 - (a) le droit d'obtenir le paiement de pénalités définies dans le Contrat ;et/ou
 - (b) le droit à ce que lesdits Services soient fournis par un tiers. Les coûts directs et justifiés supportés par le Client pour la fourniture de ces Services par ce tiers seront à la charge du Fournisseur.
- 2.4** Le paiement de ces pénalités se fera sans préjudice des autres droits et recours du Client en vertu du Contrat ou de la loi, et en particulier du droit de réclamer des dommages-intérêts et/ou de résilier le Contrat.

Sous réserve des dispositions de cet Article 2, les pénalités mentionnées ci-dessus seront plafonnées comme spécifié dans le Contrat.

3 EQUIPEMENTS, MATERIELS, OUTILS ET BIENS

Le Fournisseur maintient, à ses frais et risques, ses matériels, équipements et outils en bon état d'entretien et en conformité avec les Lois Applicables.

Le Fournisseur répare ou remplace, à ses frais, tous les matériels, équipements et outils mis à sa disposition par le Client et que le Fournisseur ou ses salariés ou ses Sous-Traitants auraient endommagés afin de les restituer dans leur état initial.

Le Fournisseur a la garde des biens et des locaux (en ce compris les matériels, équipements et outils) que le Client met à sa disposition ainsi qu'à celle de ses salariés ou de ses Sous-Traitants. Le Fournisseur restituera ces biens et locaux dans leur état initial ou tel que convenu dans le Contrat. En cas de perte ou de dommage à ces biens et locaux (ou à une partie de ceux-ci) pour quelque raison que ce soit, le Fournisseur les réparera ou les remplacera à ses frais.

4 TRANSFERT DE PROPRIETE ET DES RISQUES RELATIFS AUX SERVICES

4.1 Transfert de propriété des Eléments Associés

La propriété des Elément Associés sera transférée du Fournisseur au Client à la première des dates suivantes :

- (a) lorsque les Eléments Associés peuvent être identifiés comme se rapportant à la Commande concernée ;
- (b) lorsque le Client paie tout ou partie des Eléments Associés conformément au Contrat ; ou
- (c) lors du prononcé de la réception par le Client conformément au Contrat.

4.2 Les Eléments Associés devront être livrés libres de tout nantissement, hypothèque, sûreté, privilège, prélèvement, charge, réclamation, condition, option, ou autre restriction grevant les Eléments Associés de quelque nature que ce soit.

5 GARANTIES RELATIVES AUX SERVICES

5.1 Sauf accord contraire entre les Parties, le Fournisseur garantit la Conformité de tout Service conformément au Contrat pour une période de vingt-quatre (24) mois à compter de la date de réception d'un tel Service (la « **Période de Garantie des Services** »). En cas de non-Conformité des Services durant la Période de Garantie des Services, le Fournisseur devra réeffectuer de tels Services, sans coûts supplémentaires pour le Client.

5.2 Dans l'éventualité où tout Service devrait être ré-effectué, la Période de Garantie des Services sera étendue pour une nouvelle période de vingt-quatre (24) mois pour ces Services, à moins qu'une durée différente ne soit convenue par les Parties, à compter de la date à laquelle ces Services ont été réalisés à nouveau conformément au Contrat.

5.3 En cas de défaut du Fournisseur d'exécuter ou de ré-exécuter les Services avec la diligence requise, le Client a le droit de les faire exécuter par un tiers, après expiration d'un délai de sept (7) jours calendaires à compter de la notification écrite du Client au Fournisseur. Tous les coûts directs et justifiés supportés par le Client en lien avec l'exécution par un tiers seront facturés au Fournisseur. La réalisation par un tiers aux termes de cet Article ne libérera pas le Fournisseur de ses obligations de garantie aux termes du Contrat.

5.4 Toutefois, les garanties stipulées aux termes du présent Article 5 ne s'appliqueront pas dans la mesure où le Fournisseur que la nécessité d'une réexécution des Services résulte de l'usure normale, de dommages causés par un tiers, ou par une utilisation inappropriée par le Client, à moins que ces dommages ou cette utilisation inappropriée résultent des actes, omissions, instructions erronées ou de la négligence d'un membre quelconque du Groupe du Fournisseur.

6 RECEPTION DES SERVICES

6.1 La réception des Services et des Eléments Associés sera prononcée par le Client : (i) lorsque le Client aura inspecté ces Services et Eléments Associés pour vérifier qu'ils sont Conformes, et (ii) si les Services et Eléments Associés sont Conformes et ont été entièrement fournis.

6.2 L'exécution des Services et/ou le paiement, en tout ou partie, par le Client ne vaut pas réception des Services. La réception des Services (avec ou sans réserve) ou le refus de réception des Services est acté par écrit.

Réception sans réserve

La réception sans réserve sera prononcée lorsque le Client confirmera par écrit qu'il accepte les Services sans réserve.

Non-Conformité lors de la réception

Dans l'éventualité où le Client identifie des Services qui ne sont pas Conformés, le Client pourra soit :

- (a) procéder à la réception avec réserve(s) de ces Services, le Fournisseur devra alors effectuer les modifications nécessaires pour lever ces réserves, dans les délais indiqués par le Client.

Si, à la fin de cette période, le Fournisseur n'a pas procédé auxdites modifications de manière satisfaisante, le Client pourra :

- (i) résilier le Contrat, conformément à l'Article « Résiliation pour manquement du Fournisseur » ; ou
 - (ii) appliquer une réduction proportionnée du prix des Services concernés ; en tout état de cause, le Client aura droit aux montants mentionnés à l'Article 2.
- (b) refuser la réception et reporter la date de réception en envoyant un avis de report au Fournisseur, assorti d'une date ultime pour une nouvelle vérification de Conformité ; ou
 - (c) refuser de prononcer la réception et résilier le Contrat conformément à l'Article « Résiliation pour manquement du Fournisseur ».

6.3 Le Fournisseur restera responsable pour les défauts ou non conformités non apparents lors de la réception malgré toute inspection ou indépendamment du prononcé de la réception par le Client et ne réduira pas ou autrement n'affectera pas les obligations et garanties du Fournisseur dans le cadre du Contrat.

7 OBLIGATIONS DU FOURNISSEUR

Généralités

7.1 Le Fournisseur exécutera, et s'assurera que son Personnel, ses Sous-Traitants et leur Personnel, exécutent le Contrat :

- (a) conformément aux délais stipulés au Contrat, et, si de tels délais ne sont pas stipulés, promptement ;
- (b) conformément aux Bonnes Pratiques de la Profession, à toute Loi Applicable et Règle Obligatoire ;
- (c) en faisant preuve du degré de soin, de compétence et de diligence afin d'éviter tout dommage au Site ou aux biens du Client ; et
- (d) en tant qu'entrepreneur indépendant, ni le Fournisseur ni ses Sous-Traitants ou quelconque membre de son Personnel ne sera considéré, à quelque fin que ce soit, comme membre du Personnel du Client.

Devoir d'information

7.2 Le Fournisseur s'informerera et tiendra compte de :

- (a) tout facteur et condition externe prévisible (y compris mais sans s'y limiter, les conditions techniques) ; et
- (b) tout risque lié aux Services, y compris mais sans s'y limiter, tout risque relatif à l'hygiène, la sécurité et l'environnement

qui pourrait avoir une incidence sur l'exécution du Contrat et le Fournisseur devra informer le Client et lui fournir tout conseil visant à atténuer ces facteurs, conditions ou risques indépendamment des connaissances ou de l'expertise du Client.

Examen approfondi des informations du Client

- 7.3** Le Fournisseur devra procéder à un examen approfondi des informations fournies par ou pour le compte du Client dans le cadre de la fourniture de Services, notamment toute version mise à jour de toutes Règles Obligatoires, et le Fournisseur devra informer le Client de toute anomalie ou omission.

Le Client ne pourra être tenu responsable de l'inexactitude et de l'absence d'exhaustivité de ces informations.

Autorisations

- 7.4** Le Fournisseur garantit que lui-même et ses Sous-Traitants, conformément aux Lois Applicables, maintiendront à leurs propres frais pendant toute la Durée du Contrat, tous les enregistrements, approbations et autorisations obtenus d'autorités publiques ou d'organisations professionnelles nécessaires pour l'exécution de leurs obligations aux termes du Contrat (« **Autorisations** »). Le Client a le droit de demander au Fournisseur de lui fournir la preuve des Autorisations avant le début de toute fourniture de Services. Si une Autorisation devenait invalide pour quelque raison que ce soit, le Fournisseur en informera immédiatement le Client et ce dernier pourra résilier le Contrat conformément à l'Article 14.

Personnel

- 7.5** Le Fournisseur s'engage à affecter un Personnel qualifié, habilité et exempt de tout conflit d'intérêts pour l'exécution des Services, à assurer sa disponibilité et sa coopération pendant la durée du Contrat, tout en conservant l'autorité hiérarchique et le contrôle sur ce Personnel.

Return or destruction of Customer Data

- 7.6** Sauf disposition contraire dans le Contrat, le Fournisseur s'engage à restituer ou à détruire tout ou partie des Données Client :
- (a) à tout moment sur instruction écrite du Client ; ou
 - (b) à l'expiration ou à la résiliation du Contrat pour quelque cause que ce soit, dans un délai de 30 jours calendaires suivant l'instruction écrite du Client.

8 AUDIT ET COMPTABILITE

- 8.1** Sous réserve d'un préavis de huit (8) jours adressé au Fournisseur, le Client pourra, à tout moment, effectuer lui-même ou faire effectuer par un tiers, des audits à distance ou dans les installations respectives du Fournisseur ou de ses Sous-Traitants afin de s'assurer que le Fournisseur ou ses Sous-Traitants respectent leurs obligations aux termes du Contrat (« **Audits** »).

Le Fournisseur doit fournir au Client toute l'assistance nécessaire à la réalisation de ces Audits. Les informations obtenues lors de tout Audit ne devront être utilisées qu'à cette fin. Le Client a le droit,

au cours de tout Audit, de copier tout document et registre pour vérifier tout montant payable en vertu du Contrat.

8.2 Ces Audits n'auront pas pour effet de limiter ou d'affecter :

- (a) les obligations, responsabilités et garanties du Fournisseur aux termes du Contrat ;
- (b) le statut d'entrepreneur indépendant du Fournisseur tel que stipulé à l'Article 7.1 (d) ; et
- (c) le droit du Client de refuser tous Services.

8.3 Le Fournisseur doit fournir au Client toute l'assistance nécessaire à la réalisation de ces Audits. Les informations obtenues lors de tout Audit ne devront être utilisées qu'à cette fin. Le Client a le droit, au cours de tout Audit, de copier tout document et registre pour vérifier tout montant payable en vertu du Contrat.

8.4 Si le rapport d'audit révèle toute non-Conformité du Fournisseur avec ses obligations en vertu du Contrat, ce dernier s'engage à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai compatible avec la criticité des non-Conformités identifiées.

9 PRIX, FACTURATION ET PAIEMENTS

Paiement, prix et impôts

9.1 En contrepartie de la fourniture des Services, le Client paiera au Fournisseur les prix déterminés dans le Contrat. Ces prix sont fermes, non-révisables et incluent tous les coûts et taxes, à l'exception de la TVA.

9.2 Le Fournisseur sera seul responsable et redevable de tous taxes, impôts, prélèvements, frais, timbres, droits de douanes et cotisations de toute nature qui peuvent être mis à la charge ou prélevés par quelque autorité que ce soit auprès du Fournisseur (« **Impôts** »), ses Sociétés Apparentées, Sous-Traitants et son Personnel dans tout pays dans le cadre de l'exécution du Contrat, y compris tous impôts pour lesquels le Client pourrait être tenu d'opérer une retenue sur ses paiements au Fournisseur conformément aux Lois Applicables.

9.3 Le Fournisseur devra défendre, et tenir le Client et ses Sociétés Apparentées indemnes de toute réclamation, demande, action, procédure, jugement, sentence arbitrale (y compris les frais, coûts et dépenses juridiques raisonnables et les sommes payées à titre transactionnel), responsabilité, perte, défense, pénalité, amende et tous dommages, découlant de, se rapportant à ou en lien avec l'exécution, la mauvaise exécution ou l'inexécution du Contrat, en ce qui concerne l'Article 9.2. Le Fournisseur déclare que, dans la détermination des prix pour la fourniture de Services aux termes du Contrat, il a pris en compte tous les Impôts auxquels il est tenu conformément au présent Article.

Facturation

9.4 Le Fournisseur enverra les factures à l'adresse du Client et dans la monnaie précisée au Contrat. Ces factures devront être Conformes au Contrat (y compris à l'APPENDICE APPENDICE 1.2 des CG), à toute autre instruction du Client et aux Lois Applicables.

9.5 A la demande du Client, le Fournisseur mettra en place un système de facturation électronique, utilisant une plateforme précisée par le Client. Chaque Partie devra conclure un accord avec ce fournisseur.

9.6 Outre les mentions légales requises par les Lois Applicables, les factures devront comporter les informations suivantes :

- le numéro de TVA intracommunautaire du Fournisseur, le cas échéant ;

- les références ou le numéro d'identification du Contrat ;
- la période pour laquelle la facture est établie ;
- les montants dus par le Client ;
- la base sur laquelle les montants dus ont été calculés ;
- la description de tous les Services fournis ;
- le cas échéant, la nomenclature, le poids net en kilogrammes, le mode de transport et le pays d'origine et des Eléments Associés ;
- si nécessaire, des copies des justificatifs des montants facturés ; et
- le numéro de référence de la Commande concernée.

9.7 Le Client devra payer les factures non contestées au moyen d'un virement (ou toute autre méthode convenue) dans un délai de trente (30) jours à compter du dernier jour du mois au cours duquel la facture a été émise.

9.8 En cas de retard de paiement d'une facture non contestée due par le Client, le Fournisseur pourra appliquer à compter du terme échu de la facture, un intérêt au taux déterminé de la manière suivante :

- (a) pour les factures régies par les règles impératives du droit français sur les délais de paiement, un taux égal à trois fois le taux d'intérêt légal en vigueur en France ; ou
- (b) pour les autres factures, au taux moyen (pour la période du retard de paiement) du taux European Interbank Offered Rate à trois (3) mois (tel que publié par la Banque de France) ou un autre taux tel que convenu entre les Parties, plus un pour cent (1%).

Contestation de facture

9.9 En cas de contestation par le Client de tout ou partie d'une facture, le Client adressera au Fournisseur une notification précisant les raisons de son refus de payer. Le Client n'aura aucune obligation de payer une facture dans la mesure où le montant est contesté jusqu'à la résolution de cette contestation par les Parties. Dans ce cas, le Fournisseur devra corriger la facture et la soumettre au Client pour paiement conformément aux termes du présent Article 9.

Compensation

9.10 Le Client pourra, à sa seule discrétion, compenser les montants dus par le Fournisseur avec les montants dus par le Client aux termes du Contrat.

10 PROPRIETE INTELLECTUELLE

Eléments spécifiques

10.1 En contrepartie du paiement par le Client du prix convenu dans le Contrat, le Fournisseur cède au Client, et garantit la cession par son Personnel, ses Sous-Traitants (le cas échéant) et leur Personnel, de l'ensemble des droits de propriété intellectuelle afférents à tout élément spécifique fourni pour se conformer aux spécifications du Client, notamment, sans que cette liste soit limitative, les plans, études, maquettes, dessins, modes d'emploi, documentations techniques, manuels et documents (« **Eléments Spécifiques** »).

- 10.2** La cession prévue à l'Article 10.1 aura lieu au fur et à mesure de la création de ces Eléments Spécifiques et sera exclusive, mondiale, cessible et inclura tous les droits d'exploitation de ces Eléments Spécifiques : les droits de reproduction, représentation, traduction, adaptation, commercialisation, sur tous supports et pour toutes formes d'utilisation et d'exploitation. Ces droits seront accordés pour l'entière durée de protection des droits de propriété intellectuelle.

Eléments non spécifiques

- 10.3** Dans les cas où les Services comprennent des éléments non spécifiques, qui ne sont pas développés spécifiquement pour le Client ou pour une Société Apparentée, protégés par des droits de propriété intellectuelle (notamment, mais sans s'y limiter, des plans, manuels, documents et logiciels), fournis au Client par le Fournisseur, en contrepartie de la rémunération comprise dans le prix convenu dans le Contrat, le Fournisseur accorde au Client, à toute Société Apparentée qui pourrait être bénéficiaire du Contrat, et aux tiers agissant pour le compte du Client, un droit personnel et non-exclusif, mondial et cessible d'utiliser, de reproduire, de représenter, de traduire, de réparer et d'adapter ces éléments non-spécifiques pour les besoins du Client et toute Société Apparentée. Ces droits seront accordés pour l'entière durée de protection de droits de propriété intellectuelle et pour tous supports.
- 10.4** En cas de cession par le Client à un tiers de tout équipement ou de tout matériel ou actif, qui incorpore ou utilise un élément non spécifique, le droit d'usage du susmentionné du Client sera transféré à ce tiers, sans coût additionnel.
- 10.5** Chaque Partie conserve l'ensemble des droits qu'elle détient sur les méthodologies et méthodes d'analyse, le savoir-faire et l'expérience acquis avant l'entrée en vigueur du Contrat sous réserve, en ce qui concerne le Fournisseur, que ceux-ci n'incluent pas d'Eléments Spécifiques.

Acquisition des droits de tiers

- 10.6** Le Fournisseur fait son affaire de l'acquisition de tous les droits de propriété intellectuelle et autorisations de tiers devant participer à l'exécution du Contrat, y compris de ses employés et Sous-Traitants. Notamment, si les Services comprennent l'utilisation d'un ou plusieurs programmes informatiques appartenant à des tiers, le Fournisseur devra obtenir, à ses frais, pour le Client et les tiers impliqués dans l'exécution du Contrat, un droit d'utilisation non-exclusif de ces programmes informatiques tiers dans le cadre du Contrat.

Violation des droits de propriété intellectuelle et autres droits des tiers

- 10.7** Le Fournisseur garantit que lui-même et que ses Sous-Traitants, sont soit titulaires de tous les droits de propriété intellectuelle relatifs aux éléments fournis ou qu'ils ont obtenu toutes les licences nécessaires des tiers titulaires de ces droits de propriété intellectuelle ou d'exploitation, pour permettre au Client d'utiliser et d'exploiter librement ces éléments conformément aux dispositions de cet Article 10.

Le Fournisseur n'enfreindra pas et s'assurera que les membres de son Personnel et que ses Sous-Traitants n'enfreignent pas tout droit de tiers, et notamment leurs droits de propriété intellectuelle. Cet engagement ne trouvera pas à s'appliquer dans l'éventualité où le Fournisseur peut démontrer que la violation alléguée est imputable au Client.

- 10.8** Le Fournisseur indemniserà le Client de tous coûts, dommages, réclamations et actions judiciaires réclamés ou intentés par des tiers à raison de toute violation ou autre atteinte à leurs droits.

- 10.9** En cas de risque de réclamation ou d'action judiciaire, le Fournisseur s'engage à prendre toutes les mesures nécessaires pour mettre fin à tout risque de violation, en informera le Client et devra prendre en compte les besoins du Client.
- 10.10** Dans l'éventualité où il aura été notifié que le Client ne pourrait pas utiliser un élément faisant partie des Services sans enfreindre les droits d'un tiers, le Fournisseur devra, à ses propres frais et au choix du Client, soit remplacer l'élément concerné, soit modifier cet élément de telle sorte que la violation ou tout autre manquement cesse d'exister et que l'élément remplacé ou modifié soit Conforme aux spécifications initiales. De tels remplacements ou modifications devront être réalisés dans des délais compatibles avec les besoins du Client. Dans l'éventualité où le Fournisseur ne procéderait pas aux remplacements ou modifications, le Fournisseur devra rembourser au Client le prix des Services concernés.
- 10.11** Les dispositions ci-dessus ne porteront pas atteinte au droit du Client de demander au Fournisseur l'octroi de dommages et intérêts et/ou de résilier le Contrat conformément aux dispositions de l'Article 14.

11 CONFIDENTIALITE

- 11.1** Sont considérées comme confidentielles l'ensemble des informations ou données fournies par l'une des Parties à l'autre Partie jusqu'à ce qu'elles soient divulguées par la Partie divulgatrice ou qu'elles tombent dans le domaine public, sans violation du Contrat, et sauf si elles ont été obtenues de manière licite par une Partie auprès d'un tiers ayant le droit de divulguer ces informations.
- 11.2** La Partie réceptrice ne peut divulguer lesdites informations et données à quiconque sauf dans les cas prévus aux termes du présent article ou si elles doivent être divulguées en vertu des Lois Applicables.
- 11.3** Le Fournisseur s'engage à limiter l'accès à ces informations et données à ceux qui, parmi les membres de son Personnel, de ses Sociétés Apparentées et de ses Sous-Traitants, en ont besoin pour l'exécution du Contrat et qui sont liés par des engagements de confidentialité au moins équivalents à ceux stipulés aux termes du présent Article.
- 11.4** Le Client s'engage à limiter l'accès à ces informations et données :
- aux membres de son Personnel ;
 - à ses Sociétés Apparentées ;
 - et, à condition, qu'ils soient liés par des engagements de confidentialité au moins équivalents à ceux stipulés aux termes de cet article :
 - à ses partenaires ou partenaires potentiels ou futurs qui ont besoin d'en connaître ;
 - aux cessionnaires potentiels de bonne foi des actifs, activités ou tout autre intérêt d'un Client, dans la mesure où cela est nécessaire pour permettre l'évaluation de ces actifs, activités et/ou intérêt ;
 - aux tiers agissant au nom ou pour les besoins du Client, de ses Sociétés Apparentées ou des partenaires mentionnés ci-dessus.
- 11.5** Le Fournisseur s'engage à ne pas faire référence et à ne pas utiliser le nom commercial ou les marques déposées et/ou enregistrées du Client, pour quelque raison que soit, sans avoir au préalable obtenu l'autorisation expresse et écrite du Client.

12 RESPONSABILITE ET INDEMNISATION

Chaque Partie :

- (a) sera responsable de tout dommage (y compris tous dommages aux biens ou perte de biens, blessures ou décès) :
 - (i) qu'elle ou son Personnel cause et, s'agissant du Fournisseur, que tout Sous-Traitant cause à l'autre Partie ou à des tiers ; et/ou
 - (ii) du fait de l'exécution, la mauvaise exécution ou la non-exécution du Contrat (qu'elle soit due à une négligence, à un manquement à une obligation légale, à une faute extracontractuelle, intentionnelle ou à toute autre faute).
- (b) devra défendre, indemniser et tenir l'autre Partie et ses assureurs indemnes de tout dommage, coût et/ou responsabilité que l'autre Partie pourrait encourir à cet égard.

13 ASSURANCES

13.1 Le Fournisseur devra souscrire à ses frais pendant la durée du Contrat les assurances nécessaires, conformément aux Bonnes Pratiques de la Profession, et s'assurer que ses Sous-Traitants font de même.

Les montants de garantie indiqués ci-dessous sont des montants minimums, et ne constituent pas des limites de responsabilité.

Police d'assurance et garantie	Montant minimum assuré
Responsabilité civile « exploitation »	2.500.000 €, tous dommages confondus et par sinistre
Responsabilité civile « après travaux » et/ou « professionnelle »	2.500.000 € par sinistre
Une assurance couvrant les dommages causés à leur personnel lorsque le Fournisseur et /ou ses éventuels Sous-Traitants sont situés dans un pays où il n'existe pas de couverture sociale ;	A déterminer
Responsabilité de l'employeur	2.500.000 € par sinistre
Une assurance responsabilité civile automobile (chaque fois que le Fournisseur utilise des automobiles et du matériel automobile pour l'exécution du Contrat).	1.000.000 € par sinistre
Toutes autres polices d'assurance obligatoires dans le pays où le Site se trouve	A déterminer

13.2 Préalablement à l'exécution de tous Services et à chaque renouvellement des polices d'assurances pendant toute la durée du Contrat, le Fournisseur remettra au Client l'attestation de son assureur conforme aux montants définis ci-dessus.

13.3 Le cas échéant, les assurances de chaque Partie devront prévoir des dispositions aux termes desquelles les assureurs renoncent à leurs droits de subrogation contre l'autre Partie ou ses Sociétés Apparentées dans la limite des responsabilités et garanties d'indemnisation assumées par le Fournisseur aux termes du Contrat.

14 RESILIATION

Résiliation pour manquement du Fournisseur

14.1 Le Client peut résilier tout ou partie du Contrat en cas d'inexécution d'une obligation incombant au Fournisseur, après mise en demeure écrite restée infructueuse pendant un délai de quinze (15) jours calendaires. Le Client peut notamment résilier tout ou partie du Contrat en cas de manquement ou d'inexécution de l'obligation du Fournisseur de réaliser des Services Conformés.

14.2 Nonobstant l'Article 14.1, le Client peut résilier tout ou partie du Contrat en cas de survenance de l'un des événements suivants :

- (a) une série de manquements aux obligations du présent Contrat par le Fournisseur, tel que défini dans l'Article 14.1;
- (b) un manquement du Fournisseur dont les conséquences sont irrémédiables, notamment en cas de non-respect des Articles 3, 7.4 et 11;
- (c) si le Client apprend que le Fournisseur ne sera pas en mesure de réaliser les Services aux dates convenues au Contrat ;
- (d) le cas échéant, le Contrat cadre et/ou le contrat d'application locale a été résilié par le Client concerné pour l'une des raisons prévues dans le présent Article 14.1;
- (e) un manquement par le Fournisseur aux dispositions de toute Loi Applicable et/ou de l'une des Règles Obligatoires

La résiliation prend effet à la date indiquée dans la notification de résiliation ou, à défaut, à la date de réception par le Fournisseur de ladite notification.

14.3 En cas de résiliation du Contrat conformément aux Articles 14.1 et 14.2 :

- (a) le Client sera uniquement tenu de payer au Fournisseur, comme rémunération totale du Contrat, le montant dû pour les Services réalisés en Conformité par le Fournisseur avant la date de résiliation et réceptionnés par le Client,;
- (b) si le Client a fait exécuter tout ou partie des obligations en ayant recours à un autre fournisseur, le Client pourra facturer au Fournisseur la différence de prix entre (i) le coût supporté par le Client ; et (ii) le coût que le Client aurait dû supporter si le Fournisseur avait pleinement exécuté le Contrat, et le Client sera autorisé à recouvrer tous les coûts et dommages (y compris les dépenses de gestion supplémentaires et les frais administratifs) subis par lui en lien avec cette résiliation ; et
- (c) tout montant dû au Client conformément au présent Article 14.3 devra être payé au Client dans un délai de trente (30) jours à compter du dernier jour du mois au cours duquel la facture a été émise, faute de quoi ces montants porteront intérêts de retard au taux déterminé à l'Article 9.8 à compter de la date de cette facture jusqu'à la date à laquelle les montants dus sont payés en totalité.

Résiliation en cas de Changement de Contrôle ou d'insolvabilité du Fournisseur

14.4 Sans préjudice de tout autre droit découlant du Contrat, le Client pourra résilier le Contrat à tout moment moyennant un préavis, en cas de survenance de l'un des événements suivants :

- (a) dépôt de bilan, faillite ou règlement amiable ou prononcé du redressement ou de la liquidation judiciaire du Fournisseur ou nomination d'un administrateur provisoire, concernant le Fournisseur, sous réserve des dispositions d'ordre public applicables ;
- (b) si le Fournisseur fait l'objet d'un Changement de Contrôle.

Dans l'éventualité où le Client résilie le Contrat pour cause de Changement de Contrôle ou d'insolvabilité du Fournisseur, les dispositions de l'Article 14.3 s'appliqueront.

Résiliation à l'initiative du Client

14.5 Sans préjudice des autres dispositions du Contrat, le Client pourra, à son initiative, résilier tout ou partie du Contrat, à tout moment moyennant un préavis mais devra dans un tel cas :

- (a) payer au Fournisseur le montant dû pour les Services réalisés en Conformité par le Fournisseur avant la date de résiliation et réceptionnés par le Client;
- (b) rembourser, sur justificatif, au Fournisseur tous les coûts raisonnablement et irrévocablement encourus et payés ou engagés de bonne foi, tels que pouvant être vérifiés par des justificatifs, relativement aux Services commandés mais non fournis à la date de résiliation ;
- (c) payer au Fournisseur cinq pour cent (5%) de la différence entre (i) le prix que le Fournisseur aurait reçu s'il avait pleinement exécuté le Contrat, y compris toute Commande en cours ou partiellement exécutée, et (ii) la somme des montants d'ores et déjà payés au Fournisseur conformément aux Articles 14.5(a) et (b).

14.6 Les paiements réalisés conformément à l'Article 14.5 constitueront la rémunération finale et définitive due par le Client au Fournisseur aux termes du Contrat et le Fournisseur ne pourra prétendre à aucune indemnité relativement à la résiliation.

Résiliation pour un cas de Force Majeure prolongé

14.7 Sans préjudice de toute autre disposition du Contrat, le Client pourra résilier le Contrat à tout moment, moyennant un préavis, dans l'éventualité où un cas de Force Majeure se prolongerait sur une durée supérieure à trente (30) jours.

14.8 Dans l'éventualité où le Client résilie le Contrat aux termes de l'Article 14.7, le Client devra (a) payer au Fournisseur le montant dû pour les Services fournis par le Fournisseur et réceptionnés par le Client avant la date de résiliation ; et (b) rembourser le Fournisseur, sur justificatif, de tous les coûts raisonnablement et irrévocablement encourus et payés ou engagés de bonne foi, relativement aux Services commandés mais non fournis à la date de résiliation.

14.9 Les paiements réalisés conformément à l'Article 14.8 constitueront la rémunération finale définitive due par le Client au Fournisseur aux termes du Contrat et le Fournisseur ne pourra prétendre à aucune indemnité relativement à la résiliation.

15 FORCE MAJEURE

15.1 Aucune des Parties ne sera réputée avoir failli à ses obligations contractuelles pour tout retard ou manquement dans l'exécution de tout ou partie de ses obligations, du Contrat dans la mesure où ce retard, ce manquement résulte de / ou est la conséquence d'un cas de Force Majeure. Un cas de Force Majeure ne libère valablement la Partie qui l'invoque de ses obligations aux termes du Contrat que dans la mesure et pendant le laps de temps où cette Partie est dans l'incapacité

d'exécuter, ou est retardée dans l'exécution de, ses obligations. Chaque Partie supportera l'intégralité des coûts qui lui sont propres et qui résultent de la survenance d'un cas de Force Majeure.

15.2 La Partie affectée par un cas de Force Majeure devra immédiatement en aviser l'autre par écrit. Un tel avis devra comprendre :

- (a) des détails sur la survenance et la nature de l'évènement ou de la circonstance dont elle prétend qu'il constitue un cas de Force Majeure ; et
- (b) si possible, une estimation de la durée pendant laquelle cet évènement ou circonstance est susceptible d'avoir un impact sur ses obligations.

15.3 Toute Partie dont les obligations ont été suspendues aux termes des dispositions qui précèdent du présent Article 15 devra :

- (a) aviser l'autre Partie le plus rapidement possible après que le cas de Force Majeure a cessé ;
- (b) reprendre l'exécution de ses obligations le plus rapidement possible ;
- (c) mettre en œuvre les moyens nécessaires pour remédier à la situation le plus rapidement possible ; et
- (d) informer l'autre Partie de la date estimée de reprise de l'exécution des obligations et de la date à laquelle cette reprise a lieu.

16 CESSION

16.1 Aucun membre du Groupe du Fournisseur ne pourra céder tout ou partie de ses droits et obligations aux termes du Contrat à un tiers, sans l'accord écrit préalable du Client concerné. Le cédant restera solidairement responsable avec son cessionnaire de l'exécution complète du Contrat concerné envers le Client concerné.

16.2 Le Client pourra céder ses droits et obligations aux termes du Contrat à toute Société Apparentée, après en avoir informé le Fournisseur.

En cas de Changement de Contrôle du Fournisseur, le Fournisseur devra en informer promptement le Client.

Cession d'une Société Apparentée, d'un actif ou d'une activité

16.3 En cas de sortie de périmètre d'une Société Apparentée, d'actif ou d'activité (l' « **Entité Cédée** ») du fait de scission, cession de parts ou d'activité, fusion, Changement de Contrôle, total ou partiel, l'Entité Cédée ne pourra plus passer de Commande à compter de la date de sortie effective de l'Entité Cédée.

16.4 L'exécution des Services en cours prendra fin de plein droit à cette date. Le Fournisseur remboursera prorata temporis les paiements déjà effectués concernant l'exécution en cours non exécutée à la date de sortie effective. Le Fournisseur ne pourra prétendre à aucune indemnité au titre de la fin de ces Commandes de ce fait.

16.5 Toutefois, si la demande lui en est faite, le Fournisseur accepte par avance de poursuivre l'exécution des Services en cours pour les besoins de l'Entité Cédée pendant une période nécessaire au maintien des activités de l'Entité Cédée.

17 SOUS-TRAITANCE

- 17.1** Sous réserve des dispositions du présent Article 17 et à moins que le Client ait effectivement approuvé un ou plusieurs Sous-traitant(s) pour l'exécution des obligations du Fournisseur dans le présent Contrat, le Fournisseur ne pourra sous-traiter aucune de ses obligations au titre du Contrat.
- 17.2** Si le Fournisseur souhaite sous-traiter une partie de ses obligations aux termes du Contrat, il devra en faire la demande écrite préalable au Client en précisant :
- (a) tout détail relatif au Sous-Traitant proposé, y compris toute qualification pertinente ; et
 - (b) les obligations du Contrat que le Fournisseur souhaite sous-traiter.
- 17.3** Le Fournisseur devra interdire à ses propres Sous-Traitants de sous-traiter toute obligation aux termes du Contrat, sauf approbation du Client.
- 17.4** Le Fournisseur sera responsable de l'exécution des obligations par ses Sous-Traitants, conformément au Contrat. Le Fournisseur défendra, et tiendra le Client indemne de toutes les conséquences découlant du non-respect des exigences du Contrat par un Sous-Traitant et de toute réclamation faite par ses Sous-Traitants, leurs fournisseurs et leur Personnel respectif.

18 PRODUITS TOTALENERGIES

Sous réserve des dispositions de la Loi Applicable, le Fournisseur, dans l'exécution du Contrat, s'approvisionnera et s'engage à ce que ses Sous-Traitants s'approvisionnent, en produits et services commercialisés par le Client ou par ses Sociétés Apparentées, notamment en combustibles marins, routiers et aériens, huiles de base, fluides de forage et services puits, solvants, gaz naturel et électricité, graisses, lubrifiants, additifs, polymères, produits chimiques, joints et composants de soupapes, systèmes de batterie et systèmes photovoltaïques, à condition qu'ils soient disponibles à des prix compétitifs. Si le Fournisseur ne peut s'approvisionner en produits et services commercialisés par le Client ou par ses Sociétés Apparentées, il devra en informer le Client et justifier des raisons de cette impossibilité.

19 DISPOSITIONS DIVERSES

19.1 Notifications et remise

- (a) Toutes les notifications devant être effectuées aux termes du Contrat devront être faites par écrit et en langue française, remises en main propre, envoyées par courrier recommandé avec accusé de réception (ou par service de messagerie internationale, si la notification doit être envoyée à l'étranger) ou par message électronique avec un accusé de réception, aux adresses postales ou électroniques précisées dans le Contrat. Une Partie pourra changer son adresse postale, électronique et/ou ses coordonnées moyennant un avis préalable à l'autre Partie conformément au présent Article 19.
- (b) Une notification sera réputée ayant été remise :
 - (i) au moment de sa remise, si elle a été remise en main propre, par lettre recommandée avec accusé de réception ;
 - (ii) au moment de la réception par l'expéditeur d'un accusé de réception par le destinataire, si elle a été remise par courrier électronique.

19.2 Autonomie des Clauses

Si une stipulation du Contrat venait à être frappée de nullité en vertu d'une Loi Applicable, d'une disposition d'ordre public ou d'une décision judiciaire, elle serait réputée non écrite, cette nullité n'affectant pas la validité des autres dispositions ou l'équilibre du Contrat.

19.3 Non-renonciation

Le défaut par l'une des Parties d'exercer un droit ou un recours relativement à tout ou partie des dispositions du Contrat ne constituera pas une renonciation auxdites dispositions du Contrat.

19.4 Intégralité du Contrat

Le Contrat constitue l'intégralité de l'accord entre les Parties et annule et remplace toutes négociations, communications, déclarations et/ou accords écrits ou oraux préalables faits entre les Parties avant la Date d'Effet.

19.5 Droits cumulatifs

Les droits et recours des Parties ne seront pas limités à ceux stipulés au Contrat, et ces droits et recours seront considérés comme cumulatifs et ne seront pas exclusifs des autres droits ou recours prévus ailleurs par le Contrat, ou dans la loi à condition toutefois que le Contrat prévale toujours sur toute Loi Applicable que le Contrat contredirait ou dont le Contrat exclut expressément l'application, dans la mesure permise par la loi.

19.6 Sûretés

Le Fournisseur s'engage à ne créer ni à faire quoi que ce soit (y compris par un acte, une omission ou une négligence) qui pourrait résulter dans la création d'une sûreté ou charge sur le Site du Client, sa propriété ou ses équipements et/ou sur les Services, ou une partie de ceux-ci. Le Fournisseur déclare qu'il n'a pas créé ou causé de la manière décrite ci-dessus la création d'aucune sûreté de cette nature ou qu'il n'a rien fait de similaire avant la conclusion du Contrat.

Le Fournisseur défendra et tiendra le Client indemne de toute sûreté affectant, le Site, sa propriété et les équipements du Client et/ou les Services, ou une partie de ceux-ci, si elle a été directement créée ou causée par un acte, une omission ou une négligence du Fournisseur.

19.7 Modifications

Aucune modification du Contrat ne sera valable à moins d'avoir été fait par écrit et signée des représentants autorisés des Parties.

19.8 Dispositions survivant au Contrat

- (a) La résiliation ou l'expiration du Contrat pour quelque raison que ce soit n'affectera pas tout droit ou responsabilité qui serait né antérieurement à la résiliation ou à l'expiration du Contrat.
- (b) Sans préjudice de l'Article 19.8(a), l'arrivée du terme ou la résiliation anticipée du Contrat n'affectera pas la validité des droits et obligations qui, aux termes du Contrat ou de par leur nature, se prolongent au-delà du terme ou de cette résolution.

19.9 Documents complémentaires

Le Fournisseur devra, à ses propres frais, faire et/ou exécuter, ou faire faire et/ou exécuter, tout acte et/ou document raisonnablement demandé par le Client pour mettre en œuvre et donner plein effet aux termes du Contrat.

19.10 Exemplaires

Le Contrat peut être conclu en plusieurs exemplaires et par les Parties sur des exemplaires distincts, l'ensemble de ces exemplaires constituant un seul et même instrument.

19.11 Relation entre les Parties

Le Contrat est conclu entre Parties indépendantes. Aucune des dispositions du Contrat ne pourra être interprétée comme donnant à l'une des Parties pouvoir ou mandat pour agir au nom de l'autre Partie ou comme constituant une quelconque association, convention de mandat, partenariat, relation principal-agent ou société entre elles, ou comme créant une responsabilité solidaire entre elles.

19.12 Absence d'exclusivité

Aucune disposition du Contrat ne pourra être interprétée comme conférant une quelconque exclusivité au profit du Fournisseur.

19.13 Responsabilité solidaire

Le Client, d'une part, et toute Société Apparentée, d'autre part, ne seront pas solidairement responsables. En conséquence, chaque Société Apparentée du Client sera seul responsable de l'exécution de ses obligations envers le Fournisseur concerné.

20 DROIT DU CONTRAT ET RESOLUTION DES LITIGES

20.1 L'interprétation, l'existence et la validité du Contrat seront régies par le droit français.

20.2 Sauf à ce qu'il en soit convenu autrement dans le Contrat, les Parties conviennent de soumettre tout litige à la juridiction exclusive des tribunaux Commerciaux de Paris, France.

20.3 Les Parties excluent expressément l'application de la Convention des Nations Unies sur les contrats de vente internationale de marchandises (CVIM).

21 SANCTIONS ECONOMIQUES ET CONTROLE DES EXPORTATIONS

21.1 Le Fournisseur garantit qu'à la Date d'Effet :

- (a) aucune Lois et Réglementations sur les Sanctions n'entrave ou n'empêche le Groupe du Fournisseur d'exécuter le Contrat;
- (b) ni le Fournisseur, ni ses Sociétés Apparentées (dans la mesure où elles participent à l'exécution du Contrat), ni ses Sous-Traitants, ni ses et leurs actionnaires et directeurs ne sont des Personnes Sanctionnées ; et
- (c) le Fournisseur possède ou possédera les autorisations et licences requises pour importer et/ou exporter l'équipement du Fournisseur ou tout autre bien, équipement et technologie utilisés ou fournis pour l'exécution du Contrat en conformité avec les Lois et Réglementations sur les Sanctions.

21.2 Nonobstant toute provision contraire dans le Contrat, aucune des Parties ne saurait être obligée d'exécuter une quelconque obligation au titre du Contrat, y compris des paiements, dès lors que l'exécution de cette obligation serait contraire, violerait ou serait incompatible avec les Lois et Réglementations sur les Sanctions ou exposerait une Partie ou une de ses Sociétés Apparentées à des mesures punitives au titre de celles-ci (« **Obligations Sanctionnées** »).

21.3 Si une Loi et Réglementation sur les Sanctions constitue un cas de Force Majeure :

- (a) la Partie dont l'exécution des obligations est ainsi affectée (« **Partie Affectée** ») doit, en notifier l'autre Partie dans les délais raisonnables conformément à l'Article 21. Cette notification indiquera, a minima les informations suivantes : (i) l'identification des Lois et Réglementations sur les Sanctions qui sont considérées comme un cas de Force Majeure et la description de l'Obligation Sanctionnée et (ii) la mesure dans laquelle la Partie Affectée est empêchée d'exécuter le Contrat ; et

(b) l'une ou l'autre des Parties pourra dans ce cas :

- (i) suspendre l'Obligation Sanctionnée ; ou
- (ii) résilier le Contrat

conformément aux dispositions de l'Article 15 ou des Articles 14.7, 14.8 et 14.9.

(c) En cas de suspension partielle telle que définie au présent Article 21.3(b)(i), la Partie Affectée continuera à exécuter ses obligations au titre du Contrat dans la mesure où il ne s'agit pas d'Obligations Sanctionnées.

21.4 Nonobstant toute stipulation contraire contenue dans le Contrat, si le Fournisseur enfreint les Lois et Réglementations sur les Sanctions ou est empêché d'exécuter ses obligations en vertu du Contrat en raison d'une l'Obligation Sanctionnée qui n'équivaut pas à un cas de Force Majeure, le Client aura le droit de résilier le Contrat immédiatement par voie de notification écrite au Fournisseur. Cette résiliation prendra effet à la réception de la notification et les conséquences de cette résiliation seront celles énoncées aux Articles 14.1, 14.2 et 14.3.

21.5 L'une ou l'autre des Parties peut demander à l'autre Partie toute information requise par une Autorité de Sanctions, auquel cas cette Partie devra dûment se conformer à cette demande à moins que l'information sollicitée ne soit confidentielle ou couverte par un privilège.

21.6 Le Fournisseur doit effectuer et mettre à jour des audits de ses Sous-Traitants en utilisant des outils de vérification réputés tels que World-Check afin de s'assurer de leur respect des Lois et Réglementations sur les Sanctions et le Client se réserve le droit de demander la preuve et/ou la documentation relative à ces audits.

Le Fournisseur devra notifier dans les plus brefs délais le Client si un membre du groupe du Fournisseur ou l'un de ses actionnaires ou directeurs devient une personne sanctionnée.

APPENDICE 1.1 – REGLES DE LUTTE CONTRE LE TRAVAIL DISSIMULE

Fournisseur immatriculé en France

Le Fournisseur garantit, dans le cadre du présent Contrat, la régularité de sa situation au regard de la législation sociale. A ce titre, le Fournisseur 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.

Le Fournisseur 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 :

1 Dans tous les cas :

- 1.1** 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
- 1.2** 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.

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

- 2.1** 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
- 2.2** Une copie de la carte d'identification justifiant l'inscription au répertoire des métiers, ou
- 2.3** 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
- 2.4** Un récépissé du dépôt de déclaration auprès du Centre des Formalités des Entreprises pour les personnes en cours d'inscription.

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

- 3.1** 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.

Fournisseur non immatriculé en France

Le Fournisseur s'engage à remettre les documents et l'attestation listés ci-dessous à la signature du Contrat. Lorsque tout ou partie des Services devront être fournis en France, le Fournisseur réitérera la fourniture desdits documents et attestation tous les six (6) mois jusqu'au terme du Contrat.

Ces documents et attestation devront être soit rédigés en langue française soit envoyés avec une traduction en français.

4 Dans tous les cas :

4.1 un document indiquant son numéro d'identification individuelle ou, si le Fournisseur n'est pas obligé d'avoir un tel numéro, un document établissant son identité et son adresse ou, le cas échéant, les coordonnées de son représentant fiscal dans le pays des opérations ; et

4.2 si la législation du pays où se trouve le siège social du Fournisseur l'exige, un document émanant de l'organisme chargé de la surveillance du régime de sécurité social obligatoire et de la législation du travail applicable au Fournisseur et certifiant que le Fournisseur a déposé l'ensemble des déclarations sociales obligatoires et a effectué le paiement des cotisations et contributions associées ; et

4.3 lorsque tout ou partie des Services doivent être exécutés en France :

(a) un document attestant que le Fournisseur est en situation régulière au regard du régime de sécurité sociale et de la législation du travail conformément au règlement CE n° 883/2004 du 29 avril 2004 ou d'une convention internationale sur la sécurité sociale ou la législation du travail, ou

(b) un certificat de fourniture des déclarations sociales et de paiement des cotisations et contributions de sécurité sociale tel que prévu à l'article L. 243-15 du Code de la sécurité sociale. Dans un tel cas, ce certificat doit permettre de vérifier son authenticité via le système d'authentification prévu à l'article D. 243-15 du Code de la sécurité sociale français.

5 Lorsque l'immatriculation du Fournisseur à un registre du commerce est obligatoire dans le pays des opérations ou le pays de domiciliation :

5.1 un document émanant des autorités en charge du registre du commerce ou un document attestant d'une telle immatriculation ; ou

5.2 devis, un document publicitaire ou une correspondance professionnelle mentionnant le nom ou la dénomination sociale, l'adresse complète et la nature de l'immatriculation au registre du commerce ; ou

5.3 pour les sociétés en cours de constitution, un document de moins de six (6) mois émanant de l'organisation autorisée à procéder à l'immatriculation au registre du commerce et attestant de la demande d'immatriculation à ce registre.

6 Lorsque le Fournisseur fait appel, sur le territoire national français, à des salariés étrangers nécessitant un permis de travail en application de l'article L. 5221-2 du Code du travail français dans le cadre de l'exécution du Contrat :

6.1 une liste des noms des salariés étrangers soumis au permis de travail prévu à l'article L. 5221-2 du Code du travail français, qui devra mentionner, pour chaque salarié, la date de son embauche, sa nationalité ainsi que le type et le numéro du permis de travail.

APPENDICE 1.2 – REGLES ANTI-CORRUPTION

1 DEFINITIONS

Le terme **MEMBRE PROCHE DE LA FAMILLE D'UN AGENT PUBLIC** désigne le conjoint ou partenaire, l'un de ses enfants, l'un de ses frères et sœurs ou l'un de ses parents, le conjoint ou partenaire de l'un de ses enfants ou tout autre parent proche de son entourage familial.

Le terme **AGENT PUBLIC** désigne un agent public élu ou nommé de tout Etat ou gouvernement national, régional ou local ou toute entité, agence ou organisme d'un tel gouvernement ou Etat ou toute entreprise dans laquelle un tel gouvernement ou Etat possède, directement ou indirectement, une participation majoritaire ou de Contrôle, un responsable d'un parti politique, un candidat à des fonctions publiques et tout responsable, employé ou mandataire de toute organisation publique internationale.

2 PREVENTION DE LA CORRUPTION

2.1 En application des principes consacrés aux termes de conventions internationales et régionales relatives à la lutte contre la corruption et afin d'assurer le respect des lois anti-corruption applicables aux activités régies par le Contrat et toute autre loi anti-corruption applicable par ailleurs aux Parties ou à leurs sociétés-mères.

2.2 Le Fournisseur, pour tout ce qui attrait au Contrat et aux activités régies par le Contrat, certifie que, ni lui, ni, à sa connaissance, une personne agissant pour son compte, n'a fait ou offert, et ne fera ou n'offrira, aucun paiement, présent promesse ou tout autre avantage, que ce soit directement ou par le biais d'intermédiaires, pour l'usage ou le profit d'un Agent Public, dès lors qu'un tel paiement, présent, promesse ou avantage aurait pour but :

- (a) d'influencer un acte ou une décision de cet Agent Public ;
- (b) d'inciter cet Agent Public à accomplir ou à s'abstenir d'accomplir un Acte, en violation de ses obligations légales ;
- (c) d'obtenir un avantage indu ; ou
- (d) d'inciter cet Agent Public à faire usage de son influence en vue d'influencer tout acte ou décision de toute entité, agence ou organisme de tout gouvernement ou entreprise publique.

2.3 Le Fournisseur, pour tout ce qui attrait au Contrat et aux activités régies par le Contrat, certifie qu'il n'a pas fait ou offert, et s'engage à ne pas faire ou offrir, aucun paiement, présent, promesse ou tout avantage, que ce soit directement ou par le biais d'intermédiaires, à l'usage ou au bénéfice de toute personne (autre qu'un Agent Public), dès lors qu'un tel paiement, présent, promesse ou avantage aurait pour but d'inciter cette personne à accomplir, ou à s'abstenir d'accomplir, tout acte en violation de ses obligations légales ou d'obtenir un avantage indu, ou d'accomplir, ou à s'abstenir d'accomplir, tout acte qui violerait les lois applicables aux activités régies par le Contrat.

2.4 Le Fournisseur s'engage à imposer aux membres de son Personnel et à ses Sous-Traitants de se conformer aux obligations prévues dans la présente Appendice et à obtenir que ses Sous-Traitants s'engagent de la même façon dans leurs contrats respectifs avec tout Sous-Traitant. En particulier, le Fournisseur devra réaliser des analyses de risques anti-corruption sur tous les Sous-Traitants importants afin de s'assurer, par des investigations appropriées, que ces derniers agissent dans le respect des lois applicables en matière de prévention de la corruption. Le Client se réserve le droit

de demander la preuve et/ou la documentation utile montrant que de telles analyses de risques anti-corruption ont bien été réalisées.

- 2.5** Tous accords financiers, factures et rapport présentés au Client doivent retranscrire fidèlement et de manière raisonnablement détaillée toutes les activités et transactions effectuées dans le cadre de l'exécution du Contrat. Le Fournisseur doit également organiser et effectuer des contrôles internes adaptés afin de garantir que tous les paiements effectués dans le cadre de l'exécution du Contrat soient autorisés et en conformité avec le Contrat. Le Client se réserve le droit de réaliser lui-même, ou de faire réaliser par un représentant dûment autorisé, conformément à l'Article 8, des audits dans les locaux du Fournisseur de tous les paiements effectués par celui-ci ou pour son compte pour des Services réalisés dans le cadre du Contrat. Le Fournisseur devra coopérer totalement dans la conduite de ces audits, y compris en mettant sa comptabilité et ses archives à la disposition du Client ou des représentants dûment autorisés de celui-ci et en répondant aux questions posées par le Client relativement à l'exécution du Contrat par le Fournisseur.
- 2.6** Tous les paiements du Client au Fournisseur devront être effectués conformément aux conditions de paiement déterminées à l'Article 9 du Contrat. Les instructions de paiement notifiées par le Fournisseur, dont TotalEnergies exige qu'elles soient accompagnées d'une attestation bancaire ou d'une lettre de confort de la banque, seront considérées comme constitué une déclaration et une garantie par le Fournisseur que le compte bancaire ainsi notifié est détenu uniquement par le Fournisseur et qu'aucune personne autre que le Fournisseur ne dispose d'un droit de propriété ou d'un intérêt quelconque relativement à ce compte bancaire.
- 2.7** Le Fournisseur certifie qu'aucun Agent Public ou Membre Proche de la Famille d'un Agent Public ne détient ou ne possède, directement ou indirectement, et parts out tout autre intérêt dans le Fournisseur (autrement que par la possession de titres cotés en bourse insuffisants pour contrôler l'entité concernée), ou n'est dirigeant, administrateur ou mandataire du Fournisseur, à l'exception de toute participation, intérêt ou rôle que le Fournisseur a divulgué au Client par écrit. Cet engagement qui précède continuera à s'appliquer aussi longtemps que le Contrat restera en vigueur. Le Fournisseur devra notifier au Client rapidement et par écrit tout changement qui pourrait éventuellement contredire cet engagement. Dans tous les cas, si un Agent Public ou un Membre Proche de la Famille d'un Agent Public détient ou obtient, directement ou indirectement, des parts ou tout autre intérêt dans le Fournisseur, ou est ou devient un dirigeant, administrateur ou mandataire du Fournisseur, le Fournisseur devra prendre les mesures appropriées afin de s'assurer que cet Agent Public ou un Membre Proche de la Famille d'un Agent Public évite tout conflit d'intérêt, respecte la législation applicable selon le lieu d'exécution du Contrat prohibant les conflits d'intérêts pour les Agents Publics et respecte les dispositions anti-corruption décrites dans la présente Appendice.
- 2.8** Nonobstant ce qui précède, les Parties acceptent et reconnaissent que, dans le cas où tout Fournisseur ou Sous-Traitant est détenu par une société publique ou pourrait être considéré, que ce soit maintenant ou dans le futur, comme une entité publique ou semi-publique, il est possible qu'un Agent Public puisse occuper les fonctions de dirigeant, administrateur ou salarié de ce Fournisseur ou Sous-Traitant ou de ses filiales. Dans un tel cas, les Parties acceptent que ce Fournisseur ou ce Sous-Traitant puissent avoir un ou plusieurs dirigeants, administrateurs ou salariés qui remplissent les conditions pour être qualifiés d'Agents Publics, sous réserve que :
- (a) l'Agent Public occupe une telle fonction au sein du Fournisseur ou du Sous-Traitant de manière strictement conformément aux lois applicables à cette Partie et dans les conditions énumérées ci-dessous ;

- (b) la nomination de l'Agent Public en tant que dirigeant, administrateur ou salarié du Fournisseur ou du Sous-Traitant a été validée et approuvée par la société publique ;
- (c) tout paiement au bénéfice de ou pour le compte de l'Agent Public ait été validé et approuvé par la société publique et n'excède pas la rémunération qui serait raisonnable pour toute autre personne exerçant des fonctions similaires au sein du Fournisseur ou du Sous-Traitant ; et
- (d) cette rémunération soit strictement Conforme avec les Lois Applicables et les activités régies par le Contrat et n'ait pas pour objet d'influencer tout acte officiel, décision ou omission, ni de récompenser l'Agent Public suite à un acte officiel, décision ou omission pris par le passé.

2.9 Sans préjudice de tout autre droit ou recours que le Client pourrait avoir en application des présentes ou de la loi, notamment sans s'y limiter des dommages et intérêts pour manquements au Contrat, s'il s'avère que les engagements ou conditions prévus par la présente Appendice n'ont pas été respectés ou remplis relativement à une disposition essentielle, le Client aura le droit de :

- (a) suspendre le paiement et/ou demander le remboursement des paiements effectués en avance au titre du Contrat, et/ou
- (b) suspendre et/ou résilier le Contrat pour manquement du Fournisseur avec effet immédiat tel que prévu à l'Article 14.

APPENDICE 1.3 – PRINCIPES FONDAMENTAUX DANS LES ACHATS (PFA)

TotalEnergies inscrit le développement durable dans toutes ses dimensions au cœur de sa stratégie, de ses projets et opérations, et souhaite être une référence en matière d'engagement pour les Objectifs de Développement Durable (ODD). Nos Principes Fondamentaux dans les Achats, issus de notre Code de Conduite, constituent le socle des relations durables que nous souhaitons construire avec nos fournisseurs. Aussi, nous attendons de tous nos fournisseurs de biens et services qu'ils respectent ces principes et qu'ils s'assurent que leurs propres fournisseurs les respectent également.

Les Fournisseurs sont tenus de respecter, et de s'assurer que leurs propres fournisseurs et Sous-Traitants respectent les lois en vigueur, ainsi que les principes équivalents à ceux énoncés dans la Déclaration Universelle des Droits de l'Homme, les Conventions Fondamentales de l'Organisation Internationale du Travail, les Principes Directeurs des Nations Unies relatifs aux Entreprises et aux Droits de l'Homme, le Global Compact des Nations Unies, les Principes Volontaires sur la Sécurité et les Droits de l'Homme et Principes directeurs de l'OCDE à l'intention des Entreprises Multinationales. Des politiques et procédures efficaces doivent être mises en œuvre, en particulier en ce qui concerne les principes énoncés ci-dessous. Nous attendons aussi de nos fournisseurs qu'ils améliorent de manière continue leur performance dans ces domaines.

Principe 1 : Respecter les droits humains au travail

S'assurer que les conditions de travail et de rémunération des salariés préservent la dignité humaine et sont conformes aux principes définis par la Déclaration Universelle des Droits de l'Homme et par les Conventions Fondamentales de l'Organisation Internationale du Travail.

Interdiction et prévention du travail des enfants

- Interdire le recours aux travailleurs âgés de moins de 18 ans pour des travaux dangereux et/ou des travaux de nuit, et interdire le recours aux travailleurs âgés de moins de 15 ans, sauf lorsque la législation locale assure une plus grande protection de l'enfant.

Interdiction et prévention du travail forcé

- S'assurer qu'aucun salarié n'est contraint de travailler contre sa volonté, à travers l'usage de la violence, l'intimidation, les pressions financières ou les menaces de pénalités ou de sanctions.
- Interdire la confiscation des documents d'identité des employés. Si la législation locale exige que ces documents soient conservés, s'assurer que les employés aient un accès immédiat et automatique à ces documents.
- S'assurer qu'aucun frais de recrutement ne soit à la charge d'un salarié.

Conditions de travail, rémunération et indemnisation

- Établir un contrat de travail.
- Fournir un salaire décent et s'assurer du respect d'un nombre d'heures de travail maximum, d'un temps de repos et d'un congé parental adéquats.
- Documenter la conformité à ces exigences.

Protection de la santé, sûreté et sécurité

- Fournir un lieu de travail sain et sûr où les salariés sont protégés contre les accidents, les blessures et les maladies professionnelles.
- Lorsque qu'un logement est fourni par l'employeur, s'assurer qu'il soit sûr, propre et adéquat comme espace de vie.

Interdiction et prévention de toute discrimination et harcèlement sur le lieu de travail

- Interdire le harcèlement ainsi que les pratiques entraînant un traitement discriminatoire des employés en portant une attention particulière au recrutement, à la rémunération, aux avantages ou au licenciement.

Liberté d'expression, d'association et de convention collective, liberté de pensée, de conscience et de religion

- Permettre aux employés de choisir d'adhérer ou non à une organisation de négociation collective. Dans les pays où ce droit est restreint, s'assurer que les employés ont le droit de participer à un dialogue concernant leur situation de travail collective.

Plaintes et préoccupations

- Veiller à ce que les travailleurs puissent exprimer leurs plaintes et leurs préoccupations sans crainte de représailles.

Principe 2 : Protéger la santé, la sûreté et la sécurité

Mettre en œuvre un système de management de la santé, sûreté et sécurité : .

- Procéder à l'analyse des risques et mettre en œuvre des moyens et plans d'action adéquats pour prévenir ces risques
- Mettre en place un suivi des événements survenus dans ces domaines.
- Mettre en œuvre des plans de réponse aux incidents et des moyens d'intervention adaptés pour faire face aux différents types d'évènements que le fournisseur peut rencontrer.
- Revoir périodiquement ces politiques et mesures et mettre en place des moyens de contrôle adaptées.

Principe 3 : Agir en faveur du climat

- Mettre en place un système de management d'efficacité énergétique.
- S'efforcer de manière continue à réduire les émissions de gaz à effet de serre des opérations, des produits et/ou des services.

Principe 4 : Préserver l'environnement

Protection de l'environnement

- Limiter l'impact des activités industrielles sur l'environnement, y compris les impacts potentiels sur la qualité de l'air, les ressources en eau et les sols.

- Mettre en œuvre une approche systématique permettant de définir des objectifs environnementaux mesurables, de les atteindre et de démontrer qu'ils ont été atteints.
- Appliquer un système de gestion des risques d'atteinte à l'environnement fondé sur la hiérarchie d'atténuation Eviter-Réduire-Compenser afin d'identifier et de maîtriser l'impact environnemental des activités, des produits et/ou des services.
- Plus généralement, mettre en œuvre les améliorations nécessaires à la protection de l'environnement.

Promotion de l'économie circulaire et utilisation responsable des ressources naturelles

- S'assurer que les ressources naturelles (eau, sols, forêts...) sont utilisées de manière efficace.
- S'efforcer de manière continue à réduire la production de déchets.
- Appliquer le principe « réduire, réutiliser, recycler, valoriser ».

Protection de la biodiversité

- S'assurer qu'aucun site de production ayant un impact préjudiciable à l'environnement n'est situé dans une zone naturelle protégée incluse dans les catégories I à IV de l'Union Internationale pour la Conservation de la Nature, ou dans des zones humides désignées par la Convention Internationale de Ramsar ou dans un des Sites Naturels inscrits au Patrimoine Mondial de l'UNESCO.
- S'efforcer à réduire en continu l'impact des opérations, des produits et/ou des services sur la biodiversité en appliquant la hiérarchie d'atténuation Eviter-Réduire-Compenser.

Principe 5 : Prévenir la corruption, les conflits d'intérêts, et lutter contre la fraude

- Prévenir et rejeter la corruption sous toutes ses formes : active comme passive, privée comme publique, directe comme indirecte.
- Lutter contre la fraude.
- Eviter les conflits d'intérêts, en particulier lorsque les intérêts personnels sont susceptibles d'interférer avec les intérêts professionnels.

Principe 6 : Respecter le droit de la concurrence

- Se conformer aux règles du droit de la concurrence applicable.

Principe 7 : Promouvoir le développement économique et social

- Etablir un climat de confiance avec les Parties prenantes concernées, en instaurant un dialogue avec les communautés locales.
- Encourager les initiatives de développement local durable.
- Donner l'opportunité aux entreprises locales de développer leurs activités.

Le respect des textes et principes évoqués ci-dessus pourra faire l'objet d'un audit.

Les fournisseurs sont tenus de coopérer au processus d'audit.

APPENDICE 1.4 – HYGIENE, SECURITE ET ENVIRONNEMENT (HSE)

1 Définitions

Évènement HSE : un Incident HSE, un Presque-Accident ou une situation ou action anormale, en ce compris celles qui s'écartent d'une norme, d'une spécification, d'une procédure ou d'une règle.

Environnement : le sol, le sous-sol, l'eau, l'air, les espèces et leurs habitats, ainsi que leurs interactions.

HSE : Hygiène, Sécurité et Environnement.

Incident HSE : tout évènement survenant soudainement à une date donnée, qui cause une blessure, une maladie ou un décès, un dommage aux biens, une perte de production, ou qui nuit à l'Environnement ou à l'image professionnelle du Client et ses Société Apparentées.

Presque-Accident : tout évènement qui ne constitue pas un Incident HSE, mais qui, dans des circonstances légèrement différentes, aurait pu engendrer des conséquences identiques à celles d'un Incident HSE.

Système De Management HSE désigne une des composantes du système de management global mis en œuvre par une Partie pour gérer les risques HSE inhérents à ses activités ou à l'exécution du Contrat. Il comprend la structure organisationnelle, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources (c'est à dire les biens et équipements et le Personnel) permettant de définir, de mettre en œuvre, de revoir et de tenir à jour la politique HSE, et d'améliorer en permanence les performances HSE.

2 Dispositions Générales

2.1 Le Client accorde, et exige du Fournisseur qu'il accorde, la plus haute importance et le niveau de priorité maximal aux questions HSE à tous les niveaux de son entreprise, lors de l'exécution du Contrat.

2.2 Lors de l'exécution du Contrat, le Fournisseur prend, à ses propres frais, et s'assure que ses Sous-Traitants prennent, l'ensemble des précautions et mesures appropriées afin de (i) préserver la santé des personnes susceptibles d'être affectées par l'exécution du Contrat, (ii) garantir le maintien de hauts niveaux de sécurité lors de l'exécution du Contrat, (iii) éviter ou réduire les conséquences négatives sur l'Environnement, et (iv) protéger les biens, les équipements et le Personnel du Client.

3 Conformité HSE

3.1 Lors de l'exécution du Contrat, le Fournisseur se conforme, et s'assure que ses Sous-Traitants se conforment, à ce qui suit :

- (a) les standards HSE qui seraient attendus conformément aux Bonnes Pratiques de la Profession ;
- (b) les Règles d'Or du Client en matière de sécurité au poste travail ;
- (c) les règles, réglementations et procédures opérationnelles prévalent sur le Site, notamment s'agissant des questions HSE et des conditions d'accès au Site ;
- (d) tous processus et procédures afférents aux opérations simultanées et aux permis de travail sur le Site ;
- (e) les plans HSE, autorisations de travail et autres permis connexes (notamment, permis de travail à chaud, permis d'entrée dans un espace confiné, permis de fouille etc.) ;

(f) toute exigence spécifique indiquée dans la présente Appendice.

3.2 Le Fournisseur tiendra compte de toutes les opportunités additionnelles pour réduire les risques en termes HSE.

4 Politique HSE et Système de Management HSE du Fournisseur

4.1 Le Fournisseur maintient et met en œuvre au sein de son entreprise, une politique HSE conforme aux Bonnes Pratiques de la Profession, et à la politique HSE du Client.

4.2 Le Fournisseur maintient et met en œuvre un Système de Management HSE conforme à sa Politique HSE et au système de management HSE du Client, qui comprend toutes les procédures pertinentes pour assurer :

(a) la prévention et la réduction des risques HSE ;

la respect des dispositions de la clause «**Erreur ! Source du renvoi introuvable.**» ;

(b) le suivi et le compte-rendu au Client de la mise en œuvre des exigences de la présente Appendice, ainsi que le suivi des progrès réalisés par rapport aux objectifs HSE prédéfinis par le Fournisseur ;

(c) la qualification et l'aptitude du Personnel aux fins d'exécution des tâches requises ainsi que le bon entretien et l'adéquation des procédés, outils et matériels et équipements, aux risques HSE associés à l'exécution du Contrat.

4.3 Le Fournisseur devra justifier de sa Politique HSE et de son Système de Management HSE ainsi que de leur mise en œuvre, sur demande du Client. Dans l'hypothèse où le Système de Management HSE fait l'objet d'une certification, les informations à fournir comprendront le niveau et la durée de cette certification. Toute modification concernant cette certification devra être communiquée sans délai au Client.

4.4 Les données concernant les performances HSE du Fournisseur sur le Site pourront être utilisées librement par le Client, notamment pour des comptes rendus ou des publications.

5 Plan HSE

5.1 Avant le commencement d'exécution du Contrat, le Fournisseur doit :

(a) effectuer une visite et une inspection du Site pour en évaluer les conditions HSE ;

(b) réaliser, au moyen de méthodes d'analyse adéquates, une analyse des risques HSE couvrant tous les risques HSE susceptibles de résulter de l'exécution du Contrat. Cette analyse des risques HSE doit pleinement tenir compte de toutes les informations mises à disposition par le Client à propos des spécificités locales ayant un impact sur les aspects HSE ;

(c) au vu de ce qui précède, établir un Plan HSE conforme aux dispositions de la présente Appendice « Hygiène, Sécurité et Environnement » qui précise les exigences HSE (c'est-à-dire l'ensemble des précautions et mesures appropriées pour prévenir et réduire les risques HSE) adaptées aux spécificités du Contrat, en tenant compte de toutes les procédures du Fournisseur, nécessaires à la bonne exécution du Contrat.

5.2 Le Plan HSE doit être établi et communiqué au Client avant le commencement d'exécution du Contrat.

5.3 Toute modification du Plan HSE au cours de l'exécution du Contrat sera communiquée au Client avant que ne débutent les travaux concernés.

5.4 Le Fournisseur est responsable de la conformité de l'exécution du Contrat au Plan HSE.

6 Organisation HSE du Fournisseur

6.1 Sur demande du Client, le Fournisseur devra lui apporter la preuve qu'il dispose d'une organisation et de tous les moyens nécessaires à la bonne mise en œuvre de son Plan HSE.

6.2 Le Fournisseur s'assure que son Personnel soit informé et soucieux du respect de sa Politique HSE, de son Système de Management HSE, du Plan HSE et de l'évaluation des risques associés aux tâches qu'impose la clause « Processus de permis de travail ».

6.3 Le Fournisseur doit nommer un représentant HSE, lequel est responsable de (i) la supervision et du suivi de la mise en œuvre du Plan HSE du Fournisseur et des règles HSE en vigueur sur le Site, et (ii) des échanges avec le Client. Le Fournisseur informera le Client des coordonnées du représentant HSE.

6.4 Il appartient au Fournisseur d'assurer, à ses propres frais, la sécurité de l'ensemble des Personnels concourant à l'exécution du Contrat. Ceci implique, entre autres, la fourniture d'un équipement de protection individuelle adéquat.

6.5 Sur demande du Client, le Fournisseur devra lui apporter la preuve qu'il existe un système de communication des informations liées à la sécurité à l'occasion des rotations et changements d'équipes, et il sera responsable de sa mise en œuvre.

6.6 Le Fournisseur instaure une politique de contrôle d'aptitude médicale qu'il a la responsabilité de mettre en œuvre. Le Fournisseur doit procéder, et s'assurer que ses Sous-Traitants procèdent, en temps utile, à l'ensemble des évaluations pertinentes de nature à garantir que le Personnel participant à l'exécution du Contrat soient médicalement aptes à effectuer les tâches qui leur sont confiées.

6.7 Les dossiers médicaux des membres du Personnel du Fournisseur doivent pouvoir être consultés à tout moment par l'ensemble des autorités compétentes, durant l'exécution du Contrat.

6.8 La langue utilisée pour traiter toutes les questions HSE est de nature à assurer une bonne communication entre le Personnel du Fournisseur et celui du Client.

7 Work permit process

7.1 Le Fournisseur s'engage à respecter le processus de permis de travail applicable sur le Site.

7.2 Dans le cadre, le Fournisseur est tenu en particulier de :

- (a) dispenser à son Personnel la formation initiale sur le processus de permis de travail et assurer le maintien des connaissances sur la durée ;
- (b) s'assurer que les dangers liés aux tâches ont été formellement identifiés et que les risques y afférents ont été analysés et évalués ;
- (c) le cas échéant, veiller à ne pas débuter une quelconque prestation en vertu du Contrat sans disposer d'un permis de travail dûment validé, dès lors qu'un tel permis est requis ;

- (d) cesser dans les meilleurs délais toute intervention, et informer le Client, en cas de divergence entre les conditions indiquées dans le permis de travail et celles observées en pratique à l'occasion de l'intervention.

8 Echanges avec le Client

- 8.1** Le Fournisseur doit organiser et mettre en œuvre un système de suivi et de compte-rendu HSE à l'attention du Client. Ce système doit, entre autres, permettre de rendre compte au Client de tout Evènement HSE, comme le prévoit la clause « **Erreur ! Source du renvoi introuvable.** » ainsi que de tout risque susceptible de modifier l'analyse des risques HSE prévue dans la clause « **Erreur ! Source du renvoi introuvable.** ».
- 8.2** Si nécessaire, avant le début de l'exécution des prestations prévues au Contrat, le Client et le Fournisseur collaboreront à la mise en œuvre des mesures HSE, dans le but de prévenir les risques HSE liés aux opérations simultanées.
- 8.3** Le Fournisseur doit participer à toutes les réunions HSE organisées par le Client lors de la réunion de lancement et/ou au cours de l'exécution du Contrat.

9 Substances et matières dangereuses, déchets

- 9.1** Toutes les procédures impliquant la manipulation, le stockage, l'utilisation ou l'élimination de substances ou matières dangereuses, telles que définies par les Lois Applicables, aux fins d'exécuter le Contrat, sont traités dans le Plan HSE.
- 9.2** Le Fournisseur doit également tenir compte de toute liste de substances et matières dangereuses présentes sur le Site, qui pourrait être mise à disposition par le Client, ainsi que de toute évaluation des risques HSE y afférents.
- 9.3** Le Client se réserve le droit de refuser au Fournisseur le droit d'utiliser certaines substances ou matières dangereuses sur le Site.
- 9.4** Le Fournisseur doit s'assurer que les fiches de données de sécurité ainsi que toute autre information sur les dangers, correspondant aux substances et matières dangereuses utilisées dans le cadre de l'exécution du Contrat, puissent à tout moment être consultées par le Client sur le Site.
- 9.5** Le Fournisseur devra mettre en place un système de gestion des déchets efficace, dans le respect des Lois Applicables et toutes spécifications transmises par le Client.

10 Environnement

- 10.1** Le Fournisseur doit recenser et évaluer l'ensemble des conséquences potentielles sur l'Environnement liées à l'exécution du Contrat, et devra mettre en œuvre toutes les mesures appropriées afin de prévenir et/ou réduire ces conséquences. Ces mesures seront intégrées au Plan HSE.

11 Sous-Traitants

- 11.1** Le Fournisseur doit sélectionner ses Sous-Traitants au moyen d'un processus de qualification HSE approprié, tenant compte de leurs performances HSE et de leur aptitude à mettre en œuvre une politique HSE conforme à sa propre Politique HSE.
- 11.2** Le Fournisseur s'assure que ses Sous-Traitants maintiennent et mettent en œuvre un système de management HSE compatible avec le sien.
- 11.3** Le Fournisseur devra s'assurer que ses Sous-Traitants soient en mesure de se conformer à des exigences identiques à celles figurant dans la présente Appendice.

11.4 Le Fournisseur doit instaurer et mettre en œuvre un système permettant de vérifier les performances HSE de ses Sous-Traitants, ainsi que leur conformité aux exigences identiques à celles stipulées dans la présente Appendice « Hygiène, Sécurité et Environnement ».

11.5 Le Fournisseur doit s'assurer que les rôles et responsabilités HSE incombant respectivement au Fournisseur et aux Sous-Traitants sont clairement définis

12 Compétence et Formation

12.1 Le Fournisseur doit signaler au Client la présence de tous nouveaux membres du Personnel, c'est-à-dire tous membres du Personnel ayant moins de six (6) mois d'expérience dans le type d'activités concernées ou moins de six (6) mois de présence sur le Site, à qui il devra fournir un programme de soutien HSE approprié.

12.2 Le Fournisseur doit s'assurer que les connaissances de son Personnel en matière de HSE sont constamment tenues à jour et améliorées au moyen d'un programme de formation adéquat.

12.3 Le Fournisseur devra s'assurer que son Personnel assiste à tout programme d'intégration HSE demandé par le Client.

12.4 Avant le début des prestations objet du Contrat, le Fournisseur doit informer les membres de son Personnel qui sont affectés à l'exécution du Contrat, des risques et des mesures mises en œuvre.

12.5 Le Fournisseur s'assure que son Personnel dispose à tout moment des certificats d'aptitude nécessaire et utiles à l'exécution du Contrat.

12.6 A la demande du Client, le Fournisseur devra démontrer que son Personnel a bénéficié d'une formation HSE adéquate et pertinente pour la réalisation des prestations objets du Contrat sur le Site, laquelle devra comporter un test de connaissance portant sur les Règles d'Or du Client en matière de sécurité au travail. Le contenu de la formation HSE et les certifications seront mis à disposition du Client sur demande.

13 Préparation aux situations d'urgence

13.1 A la demande du Client, le Fournisseur lui communiquera une procédure d'intervention en cas d'urgence et tiendra dûment compte de toutes remarques formulées par le Client.

13.2 Le Fournisseur veillera à ce que son Personnel sur le Site participe à tout exercice d'urgence sur le Site qui serait organisé par le Client, ainsi qu'aux exercices de sécurité programmés.

14 Management des Evènements HSE

14.1 Le Fournisseur devra sans délai rendre compte au Client de tout Evènement HSE survenant à l'occasion de l'exécution du Contrat, eu égard à la sévérité effective ou potentielle de l'Evènement HSE.

14.2 En cas de survenance d'un Evènement HSE, le Fournisseur devra :

- (a) prendre sans délai l'ensemble des mesures correctives et préventives nécessaires, afin de réduire les effets de l'Evènement HSE et prévenir tout nouvel Evènement HSE, notamment, si nécessaire, en organisation la modification de son Plan HSE.
- (b) transmettre au Client toutes les informations pertinentes sur l'Evènement HSE et l'aider à analyser les causes de l'Evènement HSE et à en réunir les preuves ;
- (c) tenir pleinement compte des conclusions de l'analyse de ces causes dans son Système de Management HSE et le Plan HSE.

- 14.3** Tout membre du Personnel du Fournisseur qui estimerait qu'un travail en cours, faisant ou non partie des prestations prévues au titre du Contrat, présente un certain risque ou est susceptible d'engendrer un Evènement HSE, pourra en demander la suspension, jusqu'à ce que le problème soit résolu, sans encourir de sanctions.
- 14.4** Sans préjudice des dispositions de la clause « Erreur ! Source du renvoi introuvable. », le Client se réserve le droit de mener toute mesure d'intervention d'urgence.
- 14.5** En cas de maladie, de dommages corporels ou d'opérations de recherche et de sauvetage touchant le Personnel du Fournisseur, le Client s'efforcera de lui apporter son aide. Le Fournisseur tiendra le Client et ses Sociétés Apparentées indemne de tout dommage et/ou responsabilité, et l'indemnifiera de toute réclamation, notamment de tiers, né du fait ou dans le cadre de l'assistance apportée par un membre quelconque du Client et ses Sociétés Apparentées, ou de son défaut d'assistance, ou encore son incapacité à prêter une telle assistance et/ou de l'exécution de ces opérations.
- 14.6** Le Fournisseur supportera les frais liés à l'assistance apportée à son Personnel par le Client.

15 Audits HSE

- 15.1** Le Fournisseur devra prévoir dans le Plan HSE, et procéder périodiquement à, des inspections et des audits HSE internes portant sur son Personnel et les moyens mis en œuvre par ses soins durant l'exécution du Contrat. Les observations effectuées au cours de ces audits devront être communiquées au Client et se traduire par un plan d'action revue de manière régulière.
- 15.2** Le Fournisseur doit réaliser un audit périodique des performances de son Système de Management HSE et de la mise en œuvre de celui-ci.
- 15.3** Des audits pourront être réalisés par le Client conformément à la clause « Audits » sur tous les aspects HSE des prestations objets du Contrat.
- 15.4** Le Fournisseur doit procéder régulièrement à des observations de sécurité, couvrant l'ensemble des membres de son Personnel concourant aux prestations objets du présent Contrat. Les résultats de ses observations devront être communiqués au Client.

16 Nettoyage du Site

- 16.1** Dès l'achèvement de tout ou partie des prestations objets du présent Contrat sur le Site, le Fournisseur devra évacuer, à ses frais et sous sa responsabilité :
- (a) l'ensemble des moyens mis en œuvre par ses soins ;
 - (b) les installations temporaires ;
 - (c) tout reste, débris, ainsi que, plus généralement tous déchets ; et
 - (d) sauf accord contraire, tout excédent de matériaux.
- 16.2** Le Fournisseur doit nettoyer et, s'il y a lieu, remettre en état et restaurer le Site, conformément à la présente Appendice.
- 16.3** Au cas où le Fournisseur ne respecterait pas les exigences ci-dessus, le Client sera en droit, après mise en demeure du Fournisseur, de procéder (ou de faire procéder), à tout moment, à des opérations d'évacuation, de nettoyage, de remise en état et de rénovation, aux frais du Fournisseur.

17 Conséquences d'un manquement

17.1 Sans préjudice de toute autre disposition du présent Contrat, au cas où le Fournisseur ne respecterait pas l'une quelconque des dispositions de la présente Appendice « Hygiène, Sécurité et Environnement », le Client :

- (a) pourra sans délai notifier au Fournisseur qu'il a pris, ou s'apprête à prendre, aux frais du Fournisseur, toutes les mesures appropriées afin de remédier à ce manquement, dans l'hypothèse où le Fournisseur ne remplirait pas ses obligations dans les meilleurs délais ou les délais convenus ;
- (b) se réserve le droit de refuser au Fournisseur ou à tout membre du Personnel de celui-ci, l'accès au Site ou le maintien sur le Site ;
- (c) pourra suspendre l'exécution de tout ou partie des prestations objets du présent Contrat conformément aux dispositions contenues dans celui-ci le cas échéant ;
- (d) pourra mettre un terme au Contrat conformément aux dispositions contenues dans celui-ci.

17.2 En cas de décès sur le Site, le Client pourra suspendre l'exécution de tout ou partie des prestations objets du présent Contrat conformément aux dispositions contenues dans celui-ci le cas échéant.

APPENDICE 1.5 – EXIGENCES DE CYBERSECURITE

Exigences de Cybersécurité

Contrat type X (Insérer le numéro)

Exigences applicables aux contrats de type 3	:	de 1 à 13
Exigences applicables aux contrats de type 2	:	de 1 à 24
Exigences applicables aux contrats de type 1	:	de 1 à 33
Exigences supplémentaires applicables aux Contrats de type 1 avec des Ressources Spécifiques	:	de 34 à 67

NB : le modèle de Plan d'Assurances Sécurité (PAS) est à insérer en fin d'Appendice pour les contrats de type 1. Le PAS est disponible sur Agora en version française sous le n°E064 et en version anglaise sous le n°E065

Table des matières

1	TERMES ET DEFINITIONS
2	EXIGENCES APPLICABLES AUX CONTRATS DE TYPE 1, 2 ET 3
3	EXIGENCES COMPLEMENTAIRES POUR LES CONTRATS DE TYPE 1 ET 2
4	EXIGENCES COMPLEMENTAIRES POUR LES CONTRATS DE TYPE 1
5	EXIGENCES COMPLEMENTAIRES POUR LES CONTRATS DE TYPE 1 AVEC DES RESSOURCES SPECIFIQUES AU CONTRAT

PREAMBULE

Les présentes exigences de Cybersécurité fixent le cadre minimal et standard des règles qui devront être respectées par le Fournisseur et ses Sous-Traitants éventuels au titre de l'exécution du Contrat.

Ces règles doivent être précisées dans le Plan d'Assurance Sécurité pour les Contrats de type 1. Elles peuvent être précisées pour les Contrats de type 2 ou 3 dans un Plan d'Assurance Sécurité.

Les Exigences de Cybersécurité ne pourront pas prévaloir sur ou faire échec à l'application (i) de lois et réglementations applicables en matière de Cybersécurité des Systèmes et données et (ii) de règles applicables plus précises et plus strictes en matière de Cybersécurité des Systèmes et données, telles que notamment les certifications à des normes telle que ISO, ETSI ou européennes en matière de Cybersécurité applicables au Fournisseur, ses produits, ses procédures et/ou ses services, les Règles Internes et les règles autrement convenues par les Parties.

Il est rappelé que certains Systèmes d'Information et leurs Ressources, du fait de leur sensibilité, peuvent être soumis à des réglementations spécifiques, notamment en matière de confidentialité (ex : secret défense), d'obligations techniques, humaines et d'organisation, de contrôle et d'audit, de qualification des prestataires et services/moyens, de gestion d'alerte et de crise, etc. Des Règles Internes spécifiques (notamment la Politique de Sécurité des Systèmes d'Information) ainsi que des règles spécifiques contractuelles s'appliqueront et prévaudront sur les présentes Exigences de Cybersécurité.

S'agissant des Technologies de l'IA, des procédures et des dispositions supplémentaires impératives s'appliqueront dès lors que ces technologies ont vocation à être utilisées dans le cadre d'infrastructures critiques (notamment au sens de la directive (UE) 2022/2557) ou de systèmes et réseaux sensibles ou vitaux de la Compagnie ou étant soumis à des réglementations particulières en matière de Cybersécurité. Il en sera de même pour tous les systèmes d'IA à haut risque (au sens de l'AI Act). Les stipulations dans les présentes exigences relatives à l'IA ne sauraient s'y substituer ou s'appliquer par défaut.

Les références au Fournisseur doivent s'entendre comme incluant le Fournisseur et ses Sous-Traitants, les obligations du Fournisseur s'étendant aux Systèmes d'Information et aux Ressources de ses Sous-Traitants.

Termes et définitions

Les termes définis ci-après ne valent que pour les exigences de Cybersécurité – ils ne sauraient en aucun cas être utilisés ou servir de référence dans les autres documents contractuels du Contrat.

Accès à privilèges : Autorisation à accéder à une Ressource pour réaliser des opérations d'administration de la Ressource (ex : lire la configuration, modifier la configuration, exécuter une commande réservée à un administrateur, supprimer des fichiers ...).

Audit : Ensemble de vérifications permettant de s'assurer de la conformité du Fournisseur, de ses prestations ou biens, à ses obligations légales et contractuelles en matière de Cybersécurité.

Types d'Audits : organisationnels, de conformité, de configuration et techniques (intrusion, revue de codes ...)

Authentification : Procédé permettant de vérifier l'identité d'un utilisateur au Système d'Information.

Authentification forte : Authentification basée sur au moins deux (2) des éléments suivants :

- un secret connu de l'utilisateur seulement (ex : mot de passe, code PIN, etc.) ;
- un objet détenu par l'utilisateur (moyen placé sous le contrôle de la personne générant des mots de passe à usage unique, carte à puce, clé USB, etc.) ;
- une caractéristique physique de l'utilisateur (empreinte digitale, empreinte rétinienne, structure de la main, ou tout autre élément biométrique).

CERT TotalEnergies : Entité (Computer Emergency Response Team) responsable de la coordination de la réponse aux incidents informatiques et de Cybersécurité et de l'évaluation de la Cybersécurité des entités de la Compagnie et de leurs Fournisseurs.

Voir <https://totalenergies.com/cert>

Classification : La classification par le Client d'une Ressource est une information concise communiquée au Fournisseur précisant son importance et le niveau de protection approprié devant être appliqué.

Code Malveillant : Tout programme développé dans le but de nuire à ou au moyen d'un Système informatique ou d'un réseau.

Comité Sécurité (COSEC) : Instance de décision et de suivi des plans d'actions et des indicateurs Cybersécurité.

Contrat : Désigne l'ensemble des documents régissant la relation contractuelle entre le Fournisseur et le Client pour des prestations déterminées.

Cybersécurité : Ensemble des Mesures techniques et organisationnelles nécessaires et proportionnées pour protéger les Systèmes d'Information et les Ressources du Client, les Ressources Spécifiques au Contrat, les Données Client, les utilisateurs et les tierces personnes qui pourraient être impactées, contre des événements ou des actions de nature à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des Systèmes d'Informations et des Ressources susvisées ainsi que les Données Client et les services qu'ils offrent ou rendent accessibles.

Données Client : Les données, y compris à caractère personnel, auxquelles le Fournisseur a accès dans le cadre du Contrat, ainsi que les données (incluant les logs et métadonnées) générées par les Systèmes et les Ressources.

Etat de l'art : Principes, pratiques et recommandations considérés comme pertinents pour une situation standard, à un instant donné, de la sécurité des Systèmes d'Information tels que décrits notamment dans les standards (ISO, IEC) et les textes publiés par les organismes officiels (ANSSI, NIST, ENISA).

Événement : Information générée par un composant du Système d'Information faisant l'objet d'un enregistrement dans un journal.

Incident de Cybersécurité : Tout événement constaté de nature à remettre en cause la Cybersécurité ou le fonctionnement normal d'une Ressource du Système d'Information (ou d'un service fourni par la fonction SI) du Client ou d'une Ressource Spécifique au Contrat et susceptible de porter atteinte à la disponibilité, l'intégrité ou à la confidentialité de la Ressource concernée ou d'une Donnée Client.

Incident de Cybersécurité Majeur : Tout Incident de Cybersécurité ayant des conséquences, suivant les niveaux indiqués dans le Plan d'Assurance Sécurité.

Menace (de Cybersécurité) : Cause potentielle d'un Risque de Cybersécurité, qui peut nuire à un Système d'Information ou à une organisation et ses utilisateurs.

Mesure (de Cybersécurité) : Moyens pour gérer un Risque, pouvant être de nature administrative, technique, managériale ou juridique, comprenant notamment la politique, les procédures, les lignes directrices et les pratiques ou structures organisationnelles.

Niveaux de Vulnérabilité : Le CERT définit et précise les niveaux de vulnérabilité (P0, P1, Standard) et qui sont repris dans le Plan d'Assurance Sécurité ou autrement communiqués au Fournisseur.

Plan d'Assurance Sécurité (PAS) : Document décrivant les modalités d'exécution du Contrat du point de vue Cybersécurité. Ce document décrit les indicateurs Cybersécurité, l'organisation Cybersécurité et les Mesures Cybersécurité particulières mises en place.

Profil de Classification : La démarche de Classification qui consiste à attribuer une valeur correspondant à l'impact potentiel des Risques susceptibles d'affecter les Ressources analysées selon les trois critères considérés.

Chaque Ressource se voit donc attribuer, pour chacun des critères Disponibilité, Intégrité et Confidentialité, un niveau de sensibilité allant de 0 (Niveau d'impact faible) à 4 (Niveau d'impact fort).

Règles Internes : Désigne les règles du Client, notamment, toutes règles et procédures internes spécifiques au(x) Système(s) d'Information ou aux sites du Client transmises par le Client au Fournisseur ou accessibles depuis l'Intranet du Client.

Remédiation : Mise en œuvre des moyens ou Mesures de sécurité permettant de résoudre des erreurs, des failles, des défauts ou des manquements en matière de Cybersécurité.

Ressource (du Système d'Information) : Comprend tout ou partie des moyens, services et processus participant au fonctionnement du Système d'Information du Client, tels que notamment les applications, les données, les moyens techniques, les équipements, les réseaux (locaux, d'entreprise, etc.). Il est précisé que les Ressources incluent les moyens, services et processus des Fournisseurs qui participent au Système d'Information du Client, y compris les prestataires de services Cloud ou de SaaS, les prestataires en charge de services managés ou externalisés, etc.

Ressources Spécifiques au Contrat : Comprend les Ressources sous la responsabilité du Fournisseur et de ses Sous-Traitants qui sont mises en œuvre spécifiquement pour le Contrat incluant notamment les postes de travail des collaborateurs intervenant dans le cadre du Contrat et les Ressources dédiées à l'exécution du Contrat.

Risque (de Cybersécurité) : Un risque caractérisé par :

- une Menace ou une action malveillante, d'origine interne ou externe, sur des Systèmes d'Information ou les Ressources ;
- une Menace ou une action non malveillante, telle qu'une panne, une négligence ou une erreur des Systèmes d'Information ou des Ressources.

Security Operation Center (SOC) : Un centre d'opérations de sécurité (SOC) est une fonction centralisée au sein de la Compagnie qui emploie des personnes, des processus et des technologies pour surveiller et

améliorer en permanence la posture de sécurité de celle-ci tout en prévenant, détectant, analysant et répondant aux Incidents de Cybersécurité.

Systèmes : Désignent les Systèmes d'information du Client ou du Fournisseur utilisés dans le cadre du Contrat.

Système d'Information : Ensemble organisé de Ressources permettant notamment de traiter des données et fournir des services. Le Système d'Information est essentiel aux activités du Client. Il comprend le Système d'Information d'Entreprise (SIE) et le Système d'Information Industriel (SII).

Systèmes d'Information d'Entreprise (SIE) : Les SIE sont des Systèmes d'Information comprenant les services et applications destinés à la gestion de l'entreprise (bureautique, Ressources humaines, relation clients, finance, trésorerie, achats, etc.).

Systèmes d'Information Industriel (SII) : Les SII sont des Systèmes d'Information comprenant les Systèmes et les composants qui contribuent directement aux processus de production, à l'intégrité, à la sécurité et à la sûreté des sites (Systèmes de contrôle commande, gestion de laboratoire, Systèmes de gestion technique, etc.).

Technologie d'IA : Tout modèle ou système d'intelligence artificielle incorporé, utilisé et/ou exploité dans le cadre du Contrat et entrant dans le champ d'application du Règlement sur l'intelligence artificielle n°2024/1689 du 13 juin 2024 (ci-après « AI Act »).

Exigences applicables aux contrats de type 1, 2 et 3

1. Sensibiliser son Personnel à la Cybersécurité	Sensibilisation et formation à la Cybersécurité
Le Fournisseur doit conduire des actions de sensibilisation des Personnels impliqués dans l'exécution du <u>Contrat</u> (y compris les Sous-Traitants), afin de s'assurer qu'ils ont connaissance des règles de <u>Cybersécurité</u> à appliquer.	
2. Gérer les Incidents liés aux Codes Malveillants	Lutte contre les codes malveillants
Le Fournisseur doit définir et mettre en œuvre des processus et procédures de gestion des <u>Menaces</u> et des <u>Codes Malveillants</u> . Le Fournisseur est tenu de se conformer à ses obligations contractuelles et légales en matière de remontées d' <u>Incidents de Cybersécurité</u> vers le Client, y compris s'agissant de la violation de données personnelles ou non personnelles.	
3. Sécuriser les terminaux mobiles utilisés dans le cadre du Contrat	Sécurité des socles Systèmes, postes de travail et équipements nomades
Le Fournisseur doit s'assurer de l'existence de <u>Mesures</u> spécifiques et adaptées à la sécurité des terminaux mobiles (tous types d'équipement connecté) utilisés par ses Personnels (et/ou ceux de ses Sous-Traitants) dans le cadre de l'exécution du <u>Contrat</u> .	
4. Sécuriser les supports informatiques utilisés dans le cadre du Contrat	Sécurité des supports informatiques
<p>Le Fournisseur doit mettre en place des <u>Mesures</u> de protection des supports informatiques sur lesquels sont copiées, sauvegardées et/ou archivées (backup) les <u>Données Client</u> issues de l'exécution du <u>Contrat</u>.</p> <p>Les supports informatiques doivent faire l'objet d'une <u>Classification</u> formalisée et doivent être en adéquation avec le type de données copiées, sauvegardées et/ou archivées (backup).</p> <p>L'inventaire des supports informatiques doit être disponible et maintenu à jour.</p> <p>Les supports de sauvegarde et d'archivage informatique (backup) doivent être sécurisés et protégés contre des actes illicites et les <u>Risques</u> environnementaux.</p> <p>Le transport des supports informatiques doit faire l'objet d'une procédure documentée.</p>	
5. Alerter en cas d'Incident de Cybersécurité Majeur	Gestion des incidents de Cybersécurité

Les Incidents de Cybersécurité Majeurs doivent être remontés au CERT TotalEnergies dans un délai maximum de quatre (4) heures à compter du moment où le Fournisseur en a connaissance, en précisant notamment la nature et l'ampleur, avérés et potentiels, de l'Incident de Cybersécurité Majeur ainsi que toutes informations propres à permettre au Client d'apprécier les conséquences pour lui-même. Le Fournisseur collabore activement avec le Client et met à jour régulièrement ces informations et les complète.

6. Répondre aux sollicitations d'une cellule de crise du Client

Gestion des Incidents de Cybersécurité

Le Fournisseur doit disposer d'une organisation de gestion de crise lui permettant répondre aux sollicitations de la cellule de crise du Client dans les meilleurs délais.

7. Tester la continuité d'activités relatives au Contrat

Continuité d'activité

Le Fournisseur doit réaliser des tests systématiques de ses solutions organisationnelles, humaines et techniques de continuité et de reprise d'activité, à l'issue de leur mise en place ou de leur évolution, complétés par des tests et des exercices réguliers permettant d'évaluer le fonctionnement de l'ensemble des plans de continuité et de reprise d'activité qu'il a défini.

8. Privilégier l'usage des outils de collaboration

Outils collaboratifs & espaces partagés

Dans ses échanges avec le Client, le Fournisseur doit utiliser, dans toute la mesure du possible, les outils de travail collaboratif suggérés ou mis à sa disposition par le Client. Dans certains cas, notamment pour des raisons de confidentialité, le Fournisseur sera dans l'obligation d'utiliser les outils de travail collaboratif du Client.

9. Supprimer les messages électroniques et les documents liés au Contrat à la fin de celui-ci

Outils collaboratifs & espaces partagés

A moins qu'il n'en soit stipulé autrement dans un document contractuel ayant une prévalence sur les présentes exigences et sauf obligation légale impérative ou pour les besoins de la certification du produit ou service objet du Contrat, le Fournisseur doit supprimer de ses propres Ressources, incluant les Ressources Spécifiques au Contrat, les Données Client ainsi que les messages et les documents électroniques, dans un délai maximum d'un mois à compter de la cessation du Contrat pour quelque cause que ce soit.

10. Respecter les règles associées à l'usage de la messagerie et aux outils collaboratifs

Outils collaboratifs & espaces partagés

Le Fournisseur doit respecter les règles de bonnes pratiques associées à la messagerie et aux outils collaboratifs mis à sa disposition par le Client.

11. Déclaration des Technologies d'IA utilisées dans le cadre du contrat	Connaissance des Technologies d'IA
<p>Le Fournisseur devra déclarer par écrit au Client, avant toute utilisation, les Technologies d'IA qu'il souhaite utiliser dans le cadre du <u>Contrat</u>, dès sa signature puis à tout moment au cours de son exécution. Il en fera de même en cas de modification des Technologies d'IA au cours de l'exécution du <u>Contrat</u>.</p> <p>Le Client pourra s'opposer par écrit à l'utilisation de Technologies d'IA, sans avoir à se justifier et sans dédommagement ou indemnisation du Fournisseur, le <u>Contrat</u> se poursuivant dans les conditions initialement convenues et jusqu'à son terme.</p> <p>Les Technologies d'IA autorisées au jour de la signature du <u>Contrat</u> sont précisées de manière exhaustive en Appendice Description des Services.</p>	

12. Conformité des Technologies d'IA utilisées dans le cadre du Contrat	Conformité des Technologies d'IA
<p>Le Fournisseur garantit pour lui-même et pour ses Sous-Traitants que les Technologies d'IA :</p> <ul style="list-style-type: none"> - Ne comprennent aucune IA interdite (au sens de l'AI Act) et qu'aucune IA interdite n'a été utilisée antérieurement en rapport avec les Technologies d'IA dans le cadre de l'exécution du Contrat ; - Ne comprennent pas d'IA à haut risque, sauf accord préalable et écrit du Client et sous réserve de l'application de procédures, conditions contractuelles et techniques spécifiques et préalables prévues par l'AI Act ; - Sont conformes à toutes les lois applicables et notamment aux dispositions de l'AI Act, et sont mises à jour en fonction des évolutions des lois applicables, dans le respect des délais légaux, sans surcoût pour le Client ; - N'ont pas fait l'objet, au cours des six (6) derniers mois, d'interruptions résultant de l'utilisation de tout mécanisme d'urgence pour empêcher les technologies d'IA d'exécuter ou de réaliser une fonction particulière ; - Sont mises en œuvre dans le cadre de spécifications, de conception et protocoles de contrôle et de supervision stricte pour restreindre l'accès à ses Technologies d'IA et aux données d'entraînement, de test, de vérification et d'amélioration, et qu'il n'y a pas eu d'accès non autorisé à l'algorithme ou au logiciel incorporant les Technologies d'IA ou aux données d'entraînement, de test, de vérification utilisés pour former et/ou améliorer les Technologies d'IA. 	

13. Suivi des opérations réalisées sur les Technologies d'IA

Respect des obligations pesant sur les Technologies d'IA

Le Fournisseur :

- fournit au Client, toutes documentations techniques et fonctionnelles concernant les Technologies d'IA ;
- met en œuvre toutes les obligations définies à l'AI Act et en particulier les mesures d'assurance qualité, de gestion des risques, de contrôle humain, d'information, de transparence ;
- conserve les informations sous une forme lisible et facilement accessible pour le Client ou les autorités de régulation qui expliquent les opérations mises en œuvre, les résultats produits et les décisions prises ou facilitées par les Technologies d'IA.

Exigences complémentaires pour les contrats de type 1 et 2

14. Nommer un correspondant sécurité	Gouvernance de la Cybersécurité
<p>Le Fournisseur doit désigner, au sein de ses équipes, un correspondant sécurité.</p> <p>Ce correspondant sécurité est le point de contact unique en matière de sécurité pendant toute la durée du <u>Contrat</u>. Il doit être facilement joignable par le Client, de manière sécurisée et les moyens de communication doivent être établis au démarrage du <u>Contrat</u>.</p>	
15. Nommer un correspondant Remédiation	Gouvernance de la Cybersécurité
<p>Le Fournisseur doit désigner, au sein de ses équipes, un responsable chargé de l'application de la Remédiation, en relation avec le Client.</p>	
16. Produire les preuves de qualification	Certifications Cybersécurité du Fournisseur
<p>Le Fournisseur doit produire toute certification / accréditation / label / qualification et référence au <u>Client</u> étayant de sa compétence et des qualités de ses services, produits et solutions, équipements et processus en particulier dans le domaine <u>Cybersécurité</u> ainsi que celle de ses collaborateurs et de ses Sous-Traitants sur le périmètre du <u>Contrat</u>. Les preuves de qualification imposées dans un cadre réglementaire spécifique doivent également être mises à disposition.</p>	
17. Maintenir les qualifications Cybersécurité	Certifications Cybersécurité du Fournisseur
<p>Le Fournisseur est responsable de maintenir en vigueur les certifications, accréditations, qualifications et labels exigés. Les certifications <u>Cybersécurité</u> exigées en fonction du <u>Contrat</u> doivent être valides pendant au moins toute la durée du <u>Contrat</u>.</p>	
18. Notifier en cas de perte de qualification	Certifications Cybersécurité du Fournisseur
<p>Le Fournisseur doit notifier le Client dans les meilleurs délais, et au plus tard dans les sept (7) jours ouvrés à compter du moment où le Fournisseur en est informé par l'entité compétente, en cas de perte d'accréditation, de label, de qualification ou de certification, que ce soit une certification « Entreprise » ou une ou plusieurs certifications exigées s'appliquant aux Personnels, équipements, produits et solutions, services ou processus du Fournisseur ou celui de ses Sous-Traitants.</p>	

19. Former son Personnel sur les enjeux de la Cybersécurité	Sensibilisation et formation à la Cybersécurité
<p>Le Fournisseur doit s'assurer de l'acquisition, par les collaborateurs affectés à la réalisation du <u>Contrat</u> (y compris intervenants des Sous-Traitants), des connaissances et compétences requises pour l'exécution des tâches qui leurs sont confiées et des enjeux liés à la <u>Cybersécurité</u>.</p> <p>Le Fournisseur doit engager les actions de formation nécessaires au maintien à niveau des compétences pour l'ensemble des collaborateurs et intervenants concernés.</p> <p>Le Fournisseur tiendra à disposition, sur demande, la preuve de l'existence d'un programme de sensibilisation et de formation.</p>	

20. Sécuriser les postes de travail utilisés dans le cadre du Contrat	Sécurité des socles Systèmes, postes de travail et équipements nomades
<p>Le Fournisseur doit s'assurer du durcissement des postes de travail utilisés par ses Personnels (et/ou de ses Sous-Traitants) dans le cadre de la réalisation du <u>Contrat</u> afin que ces équipements ne constituent pas un vecteur d'atteinte à la sécurité des <u>Ressources</u> utilisées pour la réalisation du <u>Contrat</u> (ex : vol de matériel entraînant la divulgation d'informations confidentielles ou la perte de données essentielles, la propagation de <u>Codes Malveillants</u> ou encore l'intrusion logique et accès illicites aux <u>Ressources</u> sensibles).</p>	

21. Valider les Mesures de Cybersécurité mises en œuvre	Conception – réalisation – évolution des Ressources Spécifiques au Contrat
<p>Le Fournisseur doit procéder, avant livraison, à la vérification technique des <u>Mesures de Cybersécurité</u> mises en œuvre et restituer au Client ces résultats à l'issue de chaque campagne de contrôle. Le cas échéant, ce bilan mentionnera les écarts avec les spécifications de sécurité préalablement validées et les <u>Risques</u> résiduels de sécurité identifiés.</p>	

22. Mettre en œuvre un processus de gestion des Incidents de Cybersécurité	Gestion des Incidents de Cybersécurité
<p>Le Fournisseur doit mettre en place les moyens techniques, humains et organisationnels permettant de détecter, d'alerter, de prendre en charge et de remédier aux alertes ou aux <u>Incidents de Cybersécurité</u>, et notamment de signaler au Client les <u>Incidents de Cybersécurité</u> concernant les <u>Données Client</u> utilisées dans le cadre du <u>Contrat</u>, de réagir efficacement en fonction de la nature et gravité des incidents détectés, d'en limiter les impacts, et de résoudre rapidement et formellement tous les <u>Incidents de Cybersécurité</u>.</p>	

23. Protéger les données utilisées dans le cadre du Contrat	Outils collaboratifs & espaces partagés
<p>Le Fournisseur doit s'assurer que toutes les données et tous les documents relatifs au Client (incluant des données du Client ou celles générées par le service défini dans le <u>Contrat</u> ou les données d'inventaire) restent sur les environnements dédiés et sécurisés.</p> <p>Le transfert de données ou de documents en dehors de ces environnements, est strictement interdit. En particulier, les documents et messages échangés dans le cadre du <u>Contrat</u> ne doivent pas être communiqués à des tiers sans l'accord préalable du Client.</p> <p>Le Fournisseur doit chiffrer les messages électroniques échangés avec le Client concernant ces données, avec des <u>moyens de chiffrement conformes à l'Etat de l'art.</u></p>	

24. Respecter les bonnes pratiques de développement sécurisé	Conception – réalisation – évolution des Ressources Spécifiques au Contrat
<p>Les programmes et applications développés par le Fournisseur dans le cadre du <u>Contrat</u> doivent respecter <u>l'Etat de l'art</u> en matière de sécurité des développements informatiques et particulièrement les recommandations de l'ENISA, de l'ANSSI et de l'OWASP (Open Web Application Security Project). Ces bonnes pratiques sont décrites dans le <u>Plan d'Assurance Sécurité</u> et elles sont validées dans un <u>Comité Sécurité</u>.</p> <p>Le Fournisseur appliquera également les principes de « security by design », « security by default », en prenant également en compte, le cas échéant, les spécificités imposées par le traitement de données personnelles.</p> <p>Le Client pourra fournir un document d'exigences spécifiques sur la <u>Cybersécurité</u> selon les technologies mises en œuvre.</p>	

Exigences complémentaires pour les contrats de type 1

25. Définir les rôles et responsabilités de la Cybersécurité	Gouvernance de la Cybersécurité
<p>Le Fournisseur doit mettre en œuvre une gouvernance de la <u>Cybersécurité</u> propre à garantir le niveau de sécurité attendu par le Client et à satisfaire la totalité des exigences de <u>Cybersécurité</u>, générales et spécifiques, prévues au <u>Contrat</u> et à toutes ses Appendices.</p> <p>En cas de sous-traitance, le Fournisseur doit mettre en place sa propre gouvernance avec ses Sous-Traitants.</p> <p>Cette Gouvernance repose notamment sur la participation du Fournisseur au <u>Comité Sécurité</u> (COSEC) devant se réunir selon les modalités définies par les Parties dans un <u>Plan d'Assurance Sécurité</u> (PAS).</p> <p>Les sujets du <u>Comité Sécurité</u> porteront de façon non limitative sur l'atteinte des niveaux de sécurité attendus du Client, les <u>Incidents de Cybersécurité</u> survenus, les éventuelles dérogations sécurité impactant le Client, les <u>Incidents de Cybersécurité</u> en cours, les résultats des <u>Audits</u> ou des certifications menés.</p> <p>Les plans d'actions issus des analyses de <u>Risque</u> ou des <u>Audits</u> de Cybersécurité doivent être revus durant les <u>Comités Sécurité</u>.</p> <p>Les processus de <u>Remédiation</u>, de détection et de réaction doivent être validés par le <u>Comité Sécurité</u>.</p>	

26. Assurer un reporting sur les actions de Remédiation au périmètre du Contrat	Gestion de la Remédiation
<p>Le Fournisseur doit établir et fournir, selon les modalités et la périodicité définies dans le <u>Plan d'Assurance Sécurité</u>, les rapports pour le <u>Comité Sécurité</u>.</p>	

27. Responsabiliser les administrateurs	Administration des Ressources Spécifiques au Contrat
<p>Le Fournisseur doit veiller à ce que ses Personnels (et ceux de ses Sous-Traitants) affectés aux fonctions d'administration soient responsabilisés sur les risques et impacts pouvant découler de leurs actions réalisées grâce aux privilèges dont ils bénéficient. La démarche de responsabilisation des administrateurs doit être formalisée par écrit et être traçable.</p>	

28. Assurer le maintien en condition de sécurité des postes d'administration	Gestion des postes d'administration
<p>Le Fournisseur doit veiller à ce que les postes de travail utilisés pour l'administration soient maintenus en condition de sécurité pendant toute la durée du <u>Contrat</u>, et notamment tenus à jour et exempt de virus ou de <u>Code Malveillant</u> afin de ne pas représenter de <u>Menace</u> pour le <u>Système d'Information</u> et les Données du Client.</p>	

29. Limiter l'accès à Internet depuis les postes d'administration	Gestion des postes d'administration
<p>Les comptes des administrateurs et postes de travail utilisés pour l'administration doivent être configurés pour limiter les accès à Internet (messagerie, navigation) aux stricts besoins nécessaires à la réalisation du <u>Contrat</u>.</p>	
30. Appliquer le principe de moindre privilège pour les administrateurs	Gestion des postes d'administration
<p>Les collaborateurs du Fournisseur (et ceux de ses Sous-Traitants) disposant de droits d'administrateurs doivent avoir des comptes personnels et uniques (pas de comptes partagés) et respecter la séparation des rôles pour les actions d'administration.</p> <p>Les droits d'administration doivent être attribués et gérés en respectant le principe de moindre privilège.</p>	
31. Chiffrer les données du poste d'administration	Gestion des postes d'administration
<p>L'ensemble des supports de stockage utilisés pour l'administration du <u>Système d'Information</u> du Client doivent être chiffrés.</p> <p>Les sessions d'administration doivent faire l'objet d'une interruption automatique au bout d'une période d'inactivité déterminée et conforme à l'<u>Etat de l'art</u>.</p>	
32. Assurer la sécurité physique des postes d'administration	Gestion des postes d'administration
<p>Le Fournisseur doit veiller à mettre en œuvre des dispositifs anti-vol et de prévention des indiscrétions visuelles.</p> <p>Les opérations d'administration ne doivent en aucun cas être réalisées dans un espace ouvert au public ou visible du public.</p>	
33. Assurer un reporting sur les incidents de Cybersécurité	Gestion des incidents de Cybersécurité
<p>Le Fournisseur doit tenir à jour des états relatifs aux incidents de <u>Cybersécurité</u> et les remettre au Client selon la périodicité et avec les informations prévues dans le <u>Plan d'Assurance Sécurité</u>.</p>	

Exigences complémentaires pour les contrats de type 1 avec des Ressources Spécifiques au

Contrat

Les exigences ci-dessous s'appliquent uniquement si le Contrat comprend des ressources (équipements) sous la responsabilité du Fournisseur et de ses Sous-Traitants qui sont mises en œuvre spécifiquement pour le Contrat incluant notamment les postes de travail des collaborateurs intervenant dans le cadre du Contrat et les Ressources dédiées à l'exécution du Contrat.

34. Cartographier les Ressources Spécifiques au Contrat	Connaissance des Ressources
Le Fournisseur doit cartographier les <u>Ressources spécifiques au Contrat</u> mises en œuvre dans le cadre du <u>Contrat</u> sous la forme de schémas d'architecture et doit maintenir un inventaire détaillant les principales caractéristiques nécessaires au maintien en condition de sécurité. Cette cartographie doit être validée en <u>Comité Sécurité</u> .	

35. Tenir à jour de la cartographie des Ressources Spécifiques au Contrat	Connaissance des Ressources
Le Fournisseur doit tenir à jour la cartographie des <u>Ressources spécifiques au Contrat</u> . Les évolutions majeures doivent être présentées en <u>Comité Sécurité</u> dans un délai suffisant et raisonnable avant d'être implémentées.	

36. Classifier les Ressources Spécifiques au Contrat	Connaissance des Ressources
Le Fournisseur doit recenser les différentes <u>Ressources Spécifiques au Contrat</u> et établir, en collaboration avec le Client et sur la base du référentiel de celui-ci, une <u>Classification</u> de ces <u>Ressources</u> .	

37. Former les acteurs sur la classification des Ressources Spécifiques au Contrat	Connaissance des Ressources
Le Fournisseur doit former tout acteur impliqué dans l'utilisation ou la gestion des <u>Ressources Spécifiques au Contrat</u> sur le <u>Profil de Classification</u> des ces <u>Ressources</u> . Les administrateurs doivent maîtriser les <u>Mesures de Cybersécurité</u> applicables.	

38. Analyser les Risques de Cybersécurité sur les Ressources Spécifiques au Contrat	Gestion des Risques de Cybersécurité
Le Fournisseur doit effectuer et tenir à jour une analyse de <u>Risques de Cybersécurité</u> des <u>Ressources Spécifiques au Contrat</u> , incluant les données traitées par ces <u>Ressources</u> , suivant une méthode d'analyse convenue d'un commun accord.	

Le Fournisseur doit être en mesure de fournir à tout moment un rapport détaillé sur l'ensemble des Risques identifiés, classés par sensibilité, les moyens de prévention ou d'atténuation et faire apparaître les Risques résiduels.

39. Appliquer un plan d'action de réduction des Risques identifiés

Gestion des Risques de Cybersécurité

Le Fournisseur doit mettre en place, à ses frais, un plan d'action en lien avec l'analyse de Risques de Cybersécurité, ou les résultats d'un Audit de Cybersécurité, afin de réduire ou d'empêcher l'avènement de ces Risques de Cybersécurité ou d'en limiter les conséquences.

Le Fournisseur doit mettre en œuvre les mesures de remédiation qui s'imposeraient à la suite des notifications par le Client dans le cadre de son programme de lutte contre la fuite de données.

40. Protéger les Ressources Spécifiques au Contrat contre les Codes Malveillants

Lutte contre les codes malveillants

Le Fournisseur doit mettre en place, pour ses Ressources Spécifiques au Contrat, un dispositif de protection contre les Codes Malveillants.

41. Fournir un état périodique des moyens de lutte contre les Codes Malveillants

Lutte contre les codes malveillants

Le Fournisseur doit présenter régulièrement en Comité Sécurité un état de suivi quantitatif (complétude) et qualitatif (efficacité) des moyens de lutte contre les Codes Malveillants déployés pour protéger les Ressources Spécifiques au Contrat, selon une périodicité à définir lors des premiers Comité Sécurité.

42. Durcir les socles Systèmes des Ressources Spécifiques au Contrat

Sécurité des socles Systèmes, postes de travail et équipements nomades

Le Fournisseur doit mettre en place les Mesures techniques, humaines et organisationnelles nécessaires et pertinentes, permettant d'assurer la sécurisation des socles Systèmes (Systèmes d'exploitation, middleware, applications et services de communication et de sécurité afférents) des Ressources Spécifiques au Contrat. Ces Mesures doivent permettre de préserver la confidentialité, la disponibilité et l'intégrité des données traitées.

43. Protéger les données sur les Ressources Spécifiques au Contrat

Sécurité des socles Systèmes, postes de travail et équipements nomades

Le Fournisseur doit documenter et mettre en œuvre les moyens nécessaires et pertinents pour sécuriser l'administration, la maintenance et l'exploitation des socles Systèmes (systèmes d'exploitation, middleware, applications et services de communication et de sécurité afférents) des Ressources Spécifiques au Contrat.

44. Protéger les réseaux utilisés par les Ressources Spécifiques au Contrat	Sécurité des réseaux
<p>Le Fournisseur doit déployer et mettre à jour les <u>Mesures de sécurité</u> nécessaires, pertinentes et conformes à l'<u>Etat de l'art</u>, propres à assurer la sécurité des réseaux utilisés par les <u>Ressources Spécifiques au Contrat</u>, afin d'empêcher ou de limiter les conséquences de <u>Risques de Cybersécurité</u>.</p>	

45. Appliquer une procédure d'habilitation pour l'accès aux Ressources Spécifiques au Contrat	Contrôles d'accès logique et habilitations
<p>La gestion des accès logiques aux <u>Ressources Spécifiques au Contrat</u>, mises en œuvre par le Fournisseur pour les besoins du <u>Contrat</u>, doit être décrite dans un <u>Plan d'Assurance Sécurité</u> (le cas échéant) ou dans un document transmis au Client avant le début des Prestations/de la Fourniture et à chaque mise à jour de celui-ci.</p> <p>Les accès au <u>Système d'Information</u> du Client sont soumis aux seules règles et procédures du Client.</p>	

46. Auditer la Cybersécurité des Ressources Spécifiques au Contrat	Audits de Cybersécurité
<p>Le Fournisseur doit effectuer des <u>Audits Cybersécurité</u> des <u>Ressources Spécifiques au Contrat</u>.</p> <p>Ces <u>Audits</u> concernent essentiellement le respect des exigences définies dans ce document. Ils peuvent également porter sur les <u>Mesures de Cybersécurité</u> applicables à des réglementations spécifiques, comme celle applicable aux traitements de données personnelles.</p> <p>Ces <u>Audits</u> n'excluent pas l'application d'autres dispositions contractuelles portant sur des <u>Audits</u> des <u>Ressources</u> et <u>Systèmes d'Information</u> du Fournisseur, y compris des <u>Audits</u> de type « pen testing / red team ». Ces <u>Audits</u> sont à la charge du Fournisseur, sauf accord préalable contraire des Parties.</p>	

47. Transmettre les résultats d'Audit Cybersécurité sur les Ressources Spécifiques au Contrat	Audits de Cybersécurité
<p>Les résultats des <u>Audits</u> réalisés par le Fournisseur sur les <u>Ressources Spécifiques au Contrat</u> seront communiqués au Client. Un certificat d'<u>Audit</u>, ainsi qu'un résumé du rapport d'<u>Audit</u> et de l'avancement des actions de <u>Remédiation</u> et d'amélioration, seront remis gratuitement au Client au plus tard trente (30) jours ouvrés après la date du rapport d'<u>Audit</u>. L'ensemble des actions de <u>Remédiation</u> et d'amélioration seront à la charge du Fournisseur.</p>	

48. Remédier les vulnérabilités des Ressources Spécifiques au Contrat	Gestion de la Remédiation
--	---------------------------

Le Fournisseur doit définir et mettre en place un processus de Remédiation afin de corriger les vulnérabilités et les défauts de configuration des Ressources Spécifiques au Contrat.

49. Organiser la Remédiation dans les délais contractuels sur les Ressources Spécifiques au Contrat

Gestion de la Remédiation

Le Fournisseur doit mettre en œuvre les moyens nécessaires pour appliquer les Remédiations sur les Ressources Spécifiques au Contrat dans les délais définis dans le Plan d'Assurance Sécurité pour les Niveaux de Vulnérabilité « Critique » ou « P0 », « Urgent » ou « P1 » et Standard (par défaut). Les remédiations pour les niveaux de vulnérabilité P0 et P1 sont définies par le CERT TotalEnergies et communiquées au Fournisseur.

50. Séparer les environnements des Systèmes d'Information de production des environnements hors production

Conception – réalisation – évolution des Ressources Spécifiques au Contrat

Le Fournisseur doit s'assurer de la séparation des environnements des Systèmes d'Information de production et des Systèmes d'Information hors production. Les données de production ne doivent pas être utilisées dans les environnements hors production sauf accord préalable et écrit du Client.

51. Spécifier les Mesures de cybersécurité pour répondre aux exigences pour évolutions des Ressources Spécifiques au Contrat

Conception – réalisation – évolution des Ressources Spécifiques au Contrat

Le Fournisseur doit spécifier et documenter les dispositifs de sécurité à mettre en œuvre afin de répondre, dans le cadre des projets de conception et/ou d'évolution des Ressources Spécifiques au Contrat, aux niveaux de sécurité et de continuité de service requis par le Client.

Le Fournisseur doit alerter le Client d'une éventuelle incapacité à proposer des Mesures de Cybersécurité permettant de satisfaire aux exigences de sécurité exigées.

52. Protéger les accès physiques aux Ressources Spécifiques au Contrat

Catégorisation des zones de sécurité

Le Fournisseur doit s'assurer de la mise en place des Mesures de sécurité physique adaptées au niveau de sensibilité des Ressources Spécifiques au Contrat, y compris des données traitées dans le cadre du Contrat, et conformément à la réglementation applicable.

Le Fournisseur doit s'assurer de la protection des accès physiques aux différentes zones de sécurité dans lesquelles sont situées les Ressources Spécifiques du Contrat au moyen de dispositifs gradués et pertinents en fonction du type de zone à sécuriser.

Le Fournisseur doit s'assurer de la mise en place des Mesures de surveillance et de contrôle des dispositifs de protection des accès physiques.

53. Protection incendie des Ressources Spécifiques au Contrat	Protection contre les Risques environnementaux
<p>Le Fournisseur doit s'assurer de la mise en œuvre des <u>Mesures</u> de sécurité incendie permettant de protéger les <u>Ressources Spécifiques au Contrat</u>.</p> <p>Ces <u>Mesures</u> doivent comprendre en particulier des :</p> <ul style="list-style-type: none"> - moyens de détection des incendies ; - moyens d'extinction des incendies ; - <u>mesures</u> de vérification périodique des moyens de protection et de lutte contre les incendies ; - procédures à mettre en œuvre en cas d'incendie. <p>Le Fournisseur doit communiquer au Client la liste des <u>Mesures</u> de protection contre les incendies mises en place.</p>	

54. Protection contre les dégâts des eaux des Ressources Spécifiques au Contrat	Protection contre les Risques environnementaux
<p>Le Fournisseur doit communiquer au Client la liste des <u>Mesures</u> de protection contre les dégâts des eaux mises en place et doit s'assurer de leur mise en œuvre ainsi que leur mise à jour régulière.</p>	

55. Assurer la fourniture des services essentiels pour les Ressources Spécifiques au Contrat	Protection contre les Risques environnementaux
<p>Le Fournisseur doit s'assurer de l'installation et du bon entretien des dispositifs d'alimentation électrique, de climatisation et de protection des <u>Ressources Spécifiques au Contrat</u>.</p>	

56. Transmettre les événements permettant la supervision Cybersécurité de certaines Ressources Spécifiques au Contrat	Traçabilité et surveillance
<p>Si nécessaire, le <u>Comité Sécurité</u> peut définir les <u>Evènements</u> redoutés et scénarios de détection (journaux, évènements ou règles de détection) devant être transmis au <u>SOC</u> du Client pour qu'il soit en mesure de détecter l'occurrence. Ces événements générés par des <u>Ressources Spécifiques au Contrat</u> doivent être adressés aux <u>Systèmes</u> de collecte de logs du Client.</p>	

57. Mettre en œuvre un Security Operations Center (SOC)	Traçabilité et surveillance
<p>Le Fournisseur doit surveiller au moyen d'un <u>Security Operation Center (SOC)</u> les <u>Ressources Spécifiques au Contrat</u> qui ne sont pas intégrées au dispositif <u>SOC</u> du Client.</p> <p>Le Fournisseur doit établir, au démarrage du contrat, un protocole de communication entre son <u>SOC</u> et celui du Client.</p>	

58. Signaler les Incidents de Cybersécurité	Gestion des Incidents de Cybersécurité
<p>Le Fournisseur doit avertir le <u>CERT TotalEnergies</u> de tout <u>Incident</u> affectant ou pouvant affecter la <u>Cybersécurité des Ressources Spécifiques au Contrat</u>, dans les délais et suivant les modalités convenues contractuellement ou en application d'une réglementation, ce délai étant fixé à défaut à vingt-quatre heures au maximum à compter du moment où le Fournisseur a connaissance de l'<u>Incident de Cybersécurité</u>.</p>	
59. Transmettre les Evénements générés par un Incident Cybersécurité impactant les Ressources Spécifiques au Contrat	Traçabilité et surveillance
<p>Le Fournisseur doit transmettre au <u>Security Operation Center (SOC)</u> du Client, à première demande et dans des délais adaptés en fonction de la situation ayant générée la demande, tous les <u>Evénements</u> associés un <u>Incident Cybersécurité</u> impactant les <u>Ressources Spécifiques au Contrat</u>.</p> <p>Ces <u>Evènements</u> doivent être adressés aux moyens techniques de journalisation du Client.</p>	
60. Mettre en œuvre un Computer Emergency Response Team (CERT)	Gestion des Incidents de Cybersécurité
<p>Le Fournisseur doit décrire dans le <u>Plan d'Assurance Sécurité</u> son organisation de réponse à un <u>Incident de Cybersécurité</u>, équivalent à une organisation d'un <u>CERT (Computer Emergency Response Team)</u> pour la veille et la réaction aux <u>Incidents de Cybersécurité</u> impliquant des <u>Ressources Spécifiques au Contrat</u> qui ne sont pas intégrées aux dispositifs <u>SOC</u> et <u>CERT TotalEnergies</u>. Il désigne un point de contact apte à rendre compte au <u>CERT TotalEnergies</u>.</p> <p>Le Fournisseur doit établir un protocole de communication entre son <u>CERT</u> et celui du Client.</p>	
61. Utiliser les moyens d'Authentification mis à disposition	Administration des Ressources Spécifiques au Contrat
<p>Le Fournisseur utilisera les moyens d'<u>Authentification</u> mis à disposition par le Client pour accéder aux <u>Systèmes d'Information</u> du Client.</p> <p>A défaut, les moyens d'<u>Authentification</u> pour accéder aux <u>Ressources Spécifiques au Contrat</u> doivent être préalablement validés par le Client.</p>	
62. Protéger les mots de passe des Ressources Spécifiques au Contrat	Administration des Ressources Spécifiques au Contrat
<p>Les Personnels affectés au <u>Contrat</u> doivent protéger leurs mots de passe et leurs moyens d'<u>Authentification</u>, conformément aux méthodes validées par le <u>Comité Sécurité</u> et alerter sans délai le <u>Security Operation Center (SOC)</u> du Client en cas de compromission ou de suspicion de compromission.</p>	

63. Sécuriser les flux d'administration des Ressources Spécifiques au Contrat	Administration des Ressources Spécifiques au Contrat
<p>Le Fournisseur doit utiliser les moyens et les méthodes d'accès validés en <u>Comité Sécurité</u> pour administrer les <u>Ressources Spécifiques au Contrat</u>.</p> <p>Il s'engage à ne pas tenter de contourner les <u>Mesures de Cybersécurité</u> mises en place par le Client.</p>	

64. Tracer les actions des administrateurs sur les Ressources Spécifiques au Contrat	Administration des Ressources Spécifiques au Contrat
<p>Le Fournisseur doit s'assurer que les actions des comptes d'administration utilisés sur les <u>Ressources Spécifiques au Contrat</u> sont journalisées, conservées pour une durée par défaut de douze (12) mois glissants et que les <u>Événements</u> sont <u>Audités</u> afin de détecter des activités ou actions suspectes.</p>	

65. Assurer la disponibilité des Ressources Spécifiques au Contrat	Continuité d'activité
<p>Le Fournisseur doit évaluer les <u>Risques</u> d'indisponibilité des <u>Ressources Spécifiques au Contrat</u> pouvant être préjudiciables au Client.</p> <p>Le Fournisseur doit mettre en place les solutions (techniques, humaines et organisationnelles) visant à couvrir les scénarii d'indisponibilité identifiés, et permettant d'assurer le niveau minimum de service requis par le Client en situation de crise et la reprise du service dans des conditions conformes aux seuils de tolérance définis avec le Client.</p>	

66. Sauvegarde de secours	Continuité d'activité
<p>Le Fournisseur doit réaliser des sauvegardes de production et des sauvegardes de secours distinctes, portant sur l'ensemble des <u>Ressources Spécifiques au Contrat</u> (configuration des équipements <u>Systèmes</u>, réseaux et de télécommunications, logiciels de base, applications et <u>Données du Client</u>).</p> <p>Le Fournisseur doit externaliser les sauvegardes de secours (utilisées dans le cadre de l'exécution des plans de continuité) dans un lieu suffisamment distant du site de production pour ne pas subir les dommages d'un sinistre pouvant l'impacter. Le Fournisseur doit s'assurer de la capacité à accéder en permanence à l'ensemble des sauvegardes de secours, quel soit leur lieu d'entreposage.</p>	

67. Documenter la continuité d'activités relatives au Contrat	Continuité d'activité
<p>Le Fournisseur doit obtenir l'accord écrit du Client avant de réaliser des tests et exercices reposant sur un arrêt partiel ou complet et programmé des <u>Ressources Spécifiques au Contrat</u> ou ses autres <u>Ressources</u> nécessaires à la Fourniture (incluant ou non une bascule sur les dispositifs de secours).</p> <p>Tous les tests et exercices des dispositifs de reprise et de continuité d'activité doivent suivre des protocoles documentés par le Fournisseur. Leur exécution doit faire l'objet d'un bilan faisant état des résultats conformes aux attentes et/ou des anomalies décelées, que le Fournisseur doit transmettre au Client et qui sera commenté dans le cadre du <u>Comité Sécurité</u>.</p>	

Fin du document.