

# DOC - Modèle Accord de Confidentialité Fournisseurs

Identification du document	
Référence	<i>DOC-0026</i>
Date de dernière mise à jour	<i>18/09/2025</i>
Rédaction et vérification	<i>Florent COULON</i> Etienne GRIVELET Olivier LEUCI
Version	<i>3</i>
Etat	<i>Validé</i>
Classification	<i>Restreint</i>
Nombre de page	23

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention :** Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

# Table des matières

ACCORD DE CONFIDENTIALITE ET EXIGENCES DE SECURITE .....	4
ARTICLE 1 : OBJET DU PRESENT DOCUMENT .....	5
ARTICLE 2 : OBLIGATIONS GENERALES DU FOURNISSEUR .....	5
ARTICLE 3 : CONTRÔLES ET LITIGES .....	7
ARTICLE 4 : DUREE DE L'ACCORD .....	8
1 Exigences légales & réglementaires .....	9
2 Engagement de Responsabilité .....	9
3 Droit d'audit .....	10
4 Documentation .....	11
5 Protection des données .....	11
6 Recours à la sous-traitance .....	12
7 Equipement des personnels .....	12
8 Sensibilisation/Formation à la SSI .....	12
9 Changement chez le fournisseur .....	13
10 Installation / Déploiement Solution .....	13
11 Chiffrement .....	14
12 Gestion des accès .....	14
12.1 Autorisation des accès .....	14
13 Maintenance et Télémaintenance .....	15
14 Fin de contrat .....	16
15 Gestion des incidents de sécurité .....	16
15.1 Notification des incidents .....	16
15.2 Traitement des incidents .....	16
15.3 Investigation des incidents .....	16
16 Gestion / Correction des Vulnérabilités .....	17
17 Exigences spécifiques : Sécurité des développements fournis .....	17
17.1 Intégration de la sécurité dans le cycle de vie du développement .....	17
17.2 Évaluer les risques .....	18
17.3 Mettre en œuvre des contrôles de sécurité appropriés .....	18
17.4 Utilisation des pratiques de codage sécurisées .....	18
17.5 Mettre à jour les applications régulièrement .....	18
17.6 Sécuriser l'infrastructure .....	18
17.7 Maitrise des bibliothèques et des Framework .....	19
17.8 Habilitations .....	19
17.9 Gestion des sessions utilisateurs .....	19

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

DOC - Modèle Accord de Confidentialité Fournisseurs

17.10	Journalisation de l'application et des composants .....	19
17.11	Audits de sécurité .....	20
17.12	OWASP .....	20
17.13	Livraison des développements.....	20
17.14	Données Personnelles.....	20
18	Exigence spécifique : Sécurité dans les services en nuage .....	21
18.1	Transfert de données.....	21
18.2	Réversibilité des données .....	21
19	Liens .....	23

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

# ACCORD DE CONFIDENTIALITE ET EXIGENCES DE SECURITE

## ENTRE

La société

(Ci-après « **le fournisseur** »),

Représentée par ..... en sa qualité de ....., dûment  
habilité aux fins des présentes.

## D'UNE PART,

## ET

Le Groupement Régional d'Appui Au Développement de la e-Santé Bourgogne Franche Comté, situé 16, rue du  
Professeur Paul Milleret 25000 BESANCON

(Ci-après « **le GRADeS BFC** »),

Représenté par Nicolas LIMOGÉ, en sa qualité de Directeur, dûment habilité aux fins des présentes.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## **ARTICLE 1 : OBJET DU PRESENT DOCUMENT**

---

Ce document précise les obligations à respecter par le fournisseur en termes de confidentialité et d'exigences de sécurité.

Le champ d'application concerne :

- Tous les échanges de documents, données et/ou informations entre les parties ;
- L'ensemble du personnel du fournisseur ;
- Les sous-traitants du fournisseur.

## **ARTICLE 2 : OBLIGATIONS GENERALES DU FOURNISSEUR**

---

- Dans le cadre de ses prestations, le fournisseur mettra en œuvre toutes les mesures techniques et organisationnelles adaptées à l'état des connaissances, au contexte, aux finalités du traitement et aux risques afin de protéger les Données et prendra toutes les précautions nécessaires pour préserver la sécurité, la disponibilité, la confidentialité et l'intégrité des Données, notamment contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés.
- L'intégralité des supports et documents fournis par le GRADeS BFC au fournisseur restent la propriété du GRADeS BFC.
- Le personnel du fournisseur ainsi que le personnel de ses sous-traitants est tenu au secret professionnel (*cf. article 226-13 du code pénal*) vis-à-vis des documents, données et/ou informations dont il aura connaissance ou auxquelles il aura potentiellement accès.
- Le fournisseur s'engage à ne pas communiquer des documents, données et/ou informations à des personnes non autorisées/habilitées, qu'elles soient physiques ou morales, sauf nécessité légale ou réglementaire.
- Le fournisseur s'engage **à prendre connaissance et à respecter** les exigences de sécurité mentionnées dans l'annexe 1 et les exigences spécifiques le concernant.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

- En fin de contrat, le fournisseur est tenu de restituer **l'intégralité** des documents, données et/ou informations qui lui ont été confiés par le GRADeS BFC et de retourner signé l'attestation de suppression de données (Annexe 2 de ce document)
- Pour le fournisseur certifié ISO 27001 et Hébergeur de données ce dernier s'engage à prévenir dans un délai **de 5 jours ouvrables maximum** le GRADeS BFC de tout événement impactant leur certification (audit critique, suspension, retrait).

Le GRADeS organisera alors une réunion de crise avec le fournisseur afin de définir un plan d'actions en regard de l'évènement.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

### ARTICLE 3 : CONTRÔLES ET LITIGES

---

- Le GRADeS BFC se réserve le droit de contrôler le respect des obligations précitées par le fournisseur.
- En cas de non-respect des dispositions précitées, la responsabilité du fournisseur pourra être engagée et, le cas échéant, une plainte sera déposée par le GRADeS BFC.
- Le GRADeS BFC pourra prononcer la résiliation immédiate de(s) contrat(s) liant les deux parties, sans indemnité en faveur du fournisseur, en cas de violation du secret professionnel ou de non-respect des dispositions précitées. Cette résiliation deviendra effective quarante-cinq (45) jours après l'envoi à la partie défaillante par le GRADeS BFC d'une lettre recommandée avec accusé de réception exposant les motifs de la résiliation, à moins que dans ce délai la partie défaillante ne satisfasse à ses obligations ou n'ait apporté la preuve d'un empêchement consécutif à un cas de force majeure.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

#### **ARTICLE 4 : DUREE DE L'ACCORD**

---

Le présent accord entre en vigueur à compter du jour de sa signature par chacune des parties, et il est conclu pour **(sélectionner l'option retenue)** :

- ☐ Une durée de : .....
- ☐ La durée du projet
- ☐ La durée de(s) contrat(s) liant le fournisseur au GRADeS BFC

Il est expressément convenu entre les parties que les dispositions de cet accord de confidentialité seront maintenues **pendant une durée de 12 mois** à compter de l'expiration de celui-ci, et ce quelle qu'en soit la cause.

**Fait en France en 2 exemplaires**

GRADeS BFC,

Le fournisseur

Nom :

Fonction :

Date :

Date :

Signature :

Signature :

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*



# Annexe1 : Exigences de sécurité

## 1 Exigences légales & réglementaires

Le fournisseur doit respecter les lois et réglementations en matière de sécurité et de protection des données applicables au projet ou au service.

Le fournisseur s'engage notamment à :

- Respecter les exigences et bonnes pratiques concernant la protection des données personnelles.
- Notamment le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le guide de la sécurité des données personnelles de la CNIL.
- Respecter les exigences spécifiques au projet ou service.
  - Comme les préconisations en matière de sécurité de l'ANSSI (Agence Nationale de la Sécurité des Systèmes de l'Information), de l'ANS (Agence du Numérique en Santé) ...etc.

## 2 Engagement de Responsabilité

Le fournisseur engage sa responsabilité vis-à-vis des actions que son personnel peut effectuer dans le cadre des activités prévues au contrat/projet :

- Le personnel du fournisseur doit limiter ses actions au périmètre pour lequel il est missionné ;
- Le fournisseur doit informer son personnel des règles à respecter.
- Le fournisseur doit informer ses sous-sous-traitants des règles à respecter.

Le fournisseur s'engage à

- Formaliser et faire respecter les mêmes exigences de sécurité par ses fournisseurs engagés sur le même périmètre d'intervention au GRADeS BFC.
- Déclarer tout changement relatif à sa situation ou celle de ses sous-traitants.
- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue au contrat, avec l'accord préalable du propriétaire du document.
- Ne pas utiliser les documents et informations traités à des fins (notamment commerciales) autres que celles spécifiées au contrat.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales (sauf personnel habilité dont la liste nominative à jour sera fournie au GRADeS BFC par le fournisseur et nécessité réglementaire).
- Prendre toutes les mesures de sécurité afin d'éviter toute utilisation détournée ou frauduleuse des données et informations accédées, manipulées, traitées et/ou échangées.
- Prendre toutes les mesures de sécurité afin d'assurer la conservation et l'intégrité des documents, données et informations accédées, manipulés, traités et/ou échangés.
- Procéder à la destruction de tous fichiers ou documents en fin de contrat/prestation pour donner suite à l'action pour laquelle ils ont été nécessaires.

Le fournisseur doit :

- Avoir la capacité de fournir au GRADeS BFC, sur demande expresse, la liste nominative à jour des collaborateurs intervenant sur la prestation.
- Assurer la sécurité de sa plateforme d'intervention à distance.
- Restreindre les accès des postes concernés aux seules personnes autorisées.
- Être en mesure de déterminer, à tout instant et en toute circonstance, l'identité de toute personne qui s'est connectée sur sa plateforme.
- Mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour prévenir contre toute menace ou acte de malveillance susceptible d'affecter et/ou d'impacter la sécurité des environnements hébergés par le GRADeS BFC.

### 3 Droit d'audit

Durant la période de validité du contrat, le GRADeS BFC se réserve la possibilité de contrôler/auditer la bonne application par le fournisseur des dispositions de la présente politique, et le fournisseur s'engage à fournir tous les éléments de preuves nécessaires.

Cet audit aura lieu aux heures d'ouverture des bureaux du Titulaire et sous réserve d'en avoir informé le Titulaire au moins un mois avant sa mise en œuvre, par lettre recommandée avec accusé de réception.

Cet audit pourra être effectué par un cabinet extérieur, tenu au secret professionnel et agréé par les deux parties pour autant que celui-ci n'exerce pas également lui-même une activité concurrente de celle du Titulaire

Si le rapport d'audit fait apparaître un non-respect des obligations du Titulaire, ce dernier s'engage, dans le cadre d'un plan d'action, à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai adapté à la criticité des manquements. Un plan d'actions validé par les deux parties, incluant une clause de revoyure, sera fourni par le titulaire, dans un délai de trente (30) jours calendaires à compter de la remise du rapport d'audit. La traçabilité des corrections sera intégrée dans la procédure et/ou l'outil de suivi des incidents du fournisseur.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

La procédure d'audit ou son absence de mise en œuvre n'exonèrent d'aucune manière le fournisseur du respect de ses obligations contractuelles et ne peuvent être interprétées comme valant acceptation de la qualité des prestations effectuées.

## 4 Documentation

- Le fournisseur s'engage à fournir au GRADeS BFC toute la documentation qu'il demande ou que le fournisseur estime nécessaire.
- Le fournisseur devra maintenir la documentation fournie.

## 5 Protection des données

Le fournisseur s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) énoncée(s) dans le contrat et conformément aux instructions du GRADeS. Si le fournisseur considère qu'une instruction constitue une violation du RGPD ou tout autre disposition relative à la protection des données, il en informera immédiatement le GRADeS.
- Informer le GRADeS s'il est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis,
- Communiquer au GRADeS le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du RGPD, et de son responsable de la sécurité des systèmes d'information.
- Indiquer au GRADeS si le traitement fait l'objet d'un transfert de données hors de l'Union Européenne, le cas échéant apporter les éléments de preuve exigés par le RGPD, notamment la signature des clauses contractuelles types, BCR, et il devra réaliser le cas échéant l'AITD.

En tout état de cause aucun transfert de données hors de l'Union Européenne n'est autorisé sans validation préalable et mise en place de garanties légales adéquates (clauses contractuelles types, BCR, etc.).

- Ne Réaliser aucun transfert de données personnelles et/ou de santé sans l'accord du GRADeS BFC.
- Tracer et documenter toute copie de données qui doit être autorisée au préalable par le GRADeS
- Accéder à travers le bastion Administrateur du GRADeS pour réaliser ses missions dès que celles-ci nécessitent d'accéder à des données de santé.
- Réaliser le transfert de données de manière adaptée et sécurisée suivant le type d'informations échangés.
- Garantir la sécurité des données à caractère personnel traitées dans le cadre du présent contrat

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 6 Recours à la sous-traitance

Le fournisseur peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques.

Le fournisseur s'engage à :

- Communiquer au GRADeS la liste de ses sous-traitants impliqué et le(s) traitement associé(s).
- Durant la relation contractuelle, il informe préalablement et par écrit les équipes du GRADeS et notamment le DPD ([dpd@esante-bfc.fr](mailto:dpd@esante-bfc.fr)) et le RSSI ([rsi@esante-bfc.fr](mailto:rsi@esante-bfc.fr)) de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.
- Le GRADeS dispose d'un délai maximum de trente (30) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le GRADES n'a pas émis d'objection pendant le délai susvisé.

## 7 Equipement des personnels

Le fournisseur s'engage à mettre en œuvre les dispositifs et le paramétrage nécessaire pour prémunir ses systèmes contre les attaques virales et intrusives notamment en :

- Déployant une protection contre les virus, malware doit être installée, activée et mise à jour sur les équipements
- En chiffrant les disques durs des postes des collaborateurs
- En utilisant des systèmes d'exploitation et des logiciels supportés par l'éditeur et régulièrement mis à jour
- Limitant et séparant les droits d'administration des comptes utilisateurs.
- Interdisant le stockage local de données de santé.
- Verrouillant de manière automatique les équipements après une durée d'inactivité.

## 8 Sensibilisation/Formation à la SSI

- Le fournisseur doit s'assurer que son personnel et celui de sous-traitants le cas échéant est formé aux meilleures pratiques en matière de sécurité sur son périmètre d'intervention et est conscient des risques liés à la sécurité de l'information.
- Le fournisseur doit pouvoir fournir les preuves de ses pratiques sur première demande.
- Le fournisseur s'engage à suivre les sensibilisations que le GRADeS pourraient être amenées à dispenser à ses équipes. Les couts associés du temps passé pour suivre ses prestations ne seront pas imputés au GRADeS.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 9 Changement chez le fournisseur

Le fournisseur s'engage à :

- Notifier le GRADeS par écrit de toute modification significative des mesures techniques et/ou organisationnelles ayant un impact sur la sécurité des prestations

Les changements à notifier incluent notamment :

- L'évolution ou la suppression d'une mesure de sécurité existante
- Un changement d'architecture technique (Hébergeur, architecture, infrastructure...)
- Un changement organisationnel ayant un impact sur la sécurité (fusion, sous-traitance, externalisation...)
- Une modification des modalités contractuelles initiales concernant la sécurité.

## 10 Installation / Déploiement Solution

Le fournisseur s'engage à :

- Respecter les politiques et les procédures d'installation du GRADeS
- N'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du logiciel
- Fournir et maintenir la liste exhaustive des logiciels et éventuels équipements installés. La cartographie doit être documentée (niveau de version, prérequis, ...) et doit contenir les informations détaillant chaque logiciel ainsi que les interactions entre eux.
- Respecter le modèle de licences et la propriété intellectuelle des logiciels que son personnel installe ou met à disposition du GRADeS BFC.
- Protéger et assurer la confidentialité des données techniques (configuration, paramétrage ...) exploitées par les équipes du fournisseur.
- Fournir la matrice de flux qui décrit les flux entrants et sortants de la solution.
- Fournir le dossier d'architecture technique et dossier d'exploitation des solutions déployées
- Fournir toutes les informations d'identification qui sont nécessaires à la solution
- Les mots de passe des comptes doivent pouvoir être modifié par le GRADeS BFC.
- Les interfaces d'administration des solutions ne doivent être exposées sur internet. L'accès à ses interfaces doit passer par le bastion Administrateur.
- L'accès à ses interfaces doivent être sécurisées selon les règles de l'art.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 11 Chiffrement

- Dans le cas d'applications Web publiées sur Internet l'usage du TLS 1.2 ou plus est obligatoire.
- De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conforme à la politique de cryptographie et de chiffrement du GRADeS BFC.

## 12 Gestion des accès

### 12.1 Autorisation des accès

---

Seules les habilitations et les droits d'accès nécessaires à la réalisation des prestations des fournisseurs seront accordés à leurs employés.

Les règles d'accès, **que ce soit pour les accès physiques sur site ou pour les accès à distance**, sont les suivantes :

- Toute intervention est nécessairement planifiée au travers d'un processus impliquant une demande d'autorisation préalable par le fournisseur auprès du GRADeS BFC.
- Dans le cas d'une intervention liée à un contrat de maintenance et qui a lieu dans le cadre du maintien en condition opérationnelle des équipements ou des solutions, le fournisseur, si le degré d'urgence l'exige, contactera l'astreinte du GRADeS BFC (*le numéro de téléphone sera fourni lors l'établissement des contrats*) afin d'obtenir très rapidement un accès à la plateforme selon les modalités préconisées par l'agent du GRADeS BFC. A l'issue de l'intervention, un ticket de demande d'accès sera établi à posteriori afin de tracer ce dernier dans l'historisation des accès
- Lors d'un accès physique sur site, le personnel du fournisseur sera accompagné sur site en zone sensible par du personnel habilité du GRADeS BFC.
- Les travaux réalisés et l'éventuelle remise en état avant de quitter le site font l'objet d'un procès-verbal d'intervention envoyé au GRADeS BFC **72h ouvrées maximum** après l'intervention. Ce PV dressera le compte-rendu d'intervention en précisant au minimum, les actifs concernés par l'intervention (machines et applications) et la nature précise des actions effectuées.
- Le fournisseur s'engage à respecter les procédures et processus définis par le GRADeS BFC, ou son membre le cas échéant, pour accéder aux locaux et aux informations qui lui sont nécessaires pour remplir sa mission.
- Les règles de la politique de sécurité physique s'appliquent dans le cas où le fournisseur intervient dans les locaux du GRADeS BFC et/ou les salles d'hébergements.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 13 Maintenance et Télémaintenance

- Toutes les opérations de télémaintenance sont faites à travers **le bastion administrateur** afin d'assurer la traçabilité des actions menées et toutes les opérations effectuées sont enregistrées : toute demande de dérogation à ce moyen d'accès devra être formellement justifiée par le fournisseur et explicitement autorisée par le RSSI, le directeur du GRADeS BFC ou l'un des directeurs adjoints.
- Les accès au bastion ne se font qu'à travers des comptes individuels, nominatifs, avec de l'authentification forte et soumis à validation des équipes du GRADeS BFC.
- Le GRADeS BFC **ne donne aucun accès permanent en télémaintenance** aux environnements contenant des données de santé à caractère personnel.
- Dans le cas où l'authentification forte ne serait pas possible l'accès sera limité à une seule adresse IP publique de l'organisation.
- Le fournisseur est tenu d'informer le GRADeS BFC des comptes bastion à désactiver lors des mouvements de son personnel (départ, changement d'affectation, ...)
- Par sécurité, les comptes bastion sont automatiquement désactivés si le titulaire ne s'est pas connecté depuis **plus de 3 mois**. De plus, le GRADeS BFC effectue périodiquement des revues de contrôle des accès et comptes bastion.
- Chaque opération de maintenance menée par le fournisseur devra faire l'objet d'un descriptif clair précisant les dates, la nature des opérations et les noms des intervenants, transmis au GRADeS BFC.
- Si les champs nécessaires ne sont pas remplis de façon claire et précise, **l'accès aux ressources sera refusé**
- Par ailleurs, **un compte rendu d'intervention** devra être transmis par mail par l'intervenant responsable de l'opération de maintenance aux équipes du GRADeS ayant sollicité le fournisseur.
- Il est demandé **de planifier les interventions**, et de faire les demandes d'accès à l'avance, à l'exception des interventions correctives urgentes ou en cas de force majeure (nécessité opérationnelle).
- Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées en application du principe de minimisation des données.
- Aucun outil de prise de contrôle à distance ne peut être installé par le fournisseur
- Le rebond entre machine est autorisé uniquement à partir des machines dédiées à l'administration et mise à disposition du fournisseur
- Si le titulaire propose un système de supervision destiné au maintien en condition opérationnelle et de sécurité du système d'information, il devra en décrire précisément les catégories de données transférées. Cet usage exclusif à des fins de surveillance du maintien en condition opérationnelle et l'absence de données personnelles et ou de santé doivent être garantis.
- La solution devra utiliser des protocoles sécurisés, et passer par les dispositifs de sécurité du GRADeS BFC et être conforme au RGPD.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 14 Fin de contrat

- En fin de contrat, le fournisseur est tenu de restituer **l'intégralité** des documents, données et/ou informations qui lui ont été confiés par le GRADeS BFC et de retourner signé l'attestation de suppression de données (Annexe 2 de ce document)

Conformément à la politique d'habilitation, les droits d'accès des employés des fournisseurs sont retirés ou désactivés.

## 15 Gestion des incidents de sécurité

### 15.1 Notification des incidents

---

- Le fournisseur est tenu de signaler dans les plus brefs délais tout incident qu'il rencontrerait sur son périmètre et/ou sur les services pour lesquels il intervient.
- Concernant les incidents de sécurité le fournisseur ajoutera à la communication l'équipe RSSI du GRADeS par mail à [rssi@esante-bfc.fr](mailto:rssi@esante-bfc.fr).
- Si l'incident de sécurité entraîne une violation de données à caractères personnels le fournisseur notifiera également le DPD ([dpd@esante-bfc.fr](mailto:dpd@esante-bfc.fr)) dans les **72 heures** après en avoir pris connaissances.

Il détaillera notamment la description de la violation, les données concernées, les causes et toute documentation qu'il jugera utile.

### 15.2 Traitement des incidents

---

- Le fournisseur est tenu de prendre toutes les mesures nécessaires pour traiter les incidents qui lui sont remontés afin de minimiser les impacts.

### 15.3 Investigation des incidents

---

- Le fournisseur est tenu d'enquêter sur tous les incidents le concernant afin d'en déterminer les causes (jusqu'à la cause racine) et les conséquences.
- Dans le cas d'un incident de sécurité le fournisseur sera tenu de fournir dans les **72 heures ouvrées** après la notification :
  - Une root cause.
  - Un plan d'actions correctives et curatives.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*



## 16 Gestion / Correction des Vulnérabilités

Le fournisseur s'engage :

- A signaler au RSSI du GRADeS BFC ([rsi@esante-bfc.fr](mailto:rsi@esante-bfc.fr)) et au chef de projet toute vulnérabilité susceptible d'impacter l'activité du service, quelle que soit sa criticité, dès lors qu'il en a connaissance ;
- A traiter les risques liés à ces vulnérabilités ;
- A instruire toute vulnérabilité qui pourra lui être remontée par le GRADeS BFC.
- A effectuer un suivi et une veille des vulnérabilités sur tous les composants utilisés pour le service
- A effectuer un suivi et une veille des vulnérabilités sur tous les composants développés pour le service

Pour chaque vulnérabilité, le délai de mise en place d'un correctif devra suivre la graduation suivante :

Score CVSS	Délai de mise ne place
> à 8.9	Sous 1 mois
>= à 7 et > à 8.9	Sous 3 mois
< à 7	Prochaine mise à jour mineure de l'outil

Dans le cas où la mise en place de correctifs ne pourrait être réalisée dans les délais indiqués une réunion aura lieu entre le fournisseur et les équipes du GRADeS afin notamment :

- D'évaluer les risques
- De décider d'un plan d'action

Le fournisseur devra être en mesure de prouver que les actions effectuées ont bien corrigé les vulnérabilités identifiées.

Dans le cas où le fournisseur ne réaliserait pas les actions correctives sous sa responsabilité, il sera tenu responsable de toutes les conséquences liées à l'exploitation de la vulnérabilité en question, et le GRADeS BFC pourra prendre toutes les mesures nécessaires pour protéger les données hébergées et/ou ses actifs.

## 17 Exigences spécifiques : Sécurité des développements fournis

### 17.1 Intégration de la sécurité dans le cycle de vie du développement

- Le fournisseur devra s'assurer que la sécurité soit considérée dès la phase de planification du projet et intégrée à toutes les phases du cycle de vie du développement, y compris la conception, le développement, les tests, la mise en production et la maintenance.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

DOC - Modèle Accord de Confidentialité Fournisseurs

## 17.2 Évaluer les risques

---

- Il devra évaluer les risques pour identifier les menaces et vulnérabilités potentielles qui pourraient affecter l'application. Cette évaluation doit être documentée et mise à jour régulièrement.

## 17.3 Mettre en œuvre des contrôles de sécurité appropriés

---

- Des contrôles de sécurité appropriés doivent être mis en œuvre pour atténuer les risques identifiés.
- Le fournisseur s'engage à mettre en place ces contrôles pouvant inclure des mesures techniques, telles que le chiffrement des données, ou des mesures administratives, telles que la mise en place d'une politique de mots de passe forte.
- Il fournira une liste exhaustive des contrôles mis en place.

## 17.4 Utilisation des pratiques de codage sécurisées

---

- Les développeurs doivent suivre des pratiques de codage sécurisées pour réduire le risque d'introduire des vulnérabilités dans le code.
- Ces pratiques incluent, par exemple, l'utilisation de bibliothèques sécurisées, le test des entrées des utilisateurs et la validation des données.
- Les équipes de développement du fournisseur doivent être formés au développement sécurisé et notamment respecter les bonnes pratiques de sécurité des langages utilisés.
- Des revues de code devront être régulièrement effectuées.
- Les développeurs ne doivent en aucun cas utiliser du code provenant d'une source inconnue ou qui n'a pas été vérifiée (forums, internet, etc.). De plus, l'utilisation d'un code sous copyright est également prohibée, ou doit comporter une description contractuelle.
- Le « codage en dur » d'identifiants dans le code source est prohibé.

Les identifiants ne devant pas être « codés en dur » peuvent être (Liste Non exhaustive) :

- Nom d'utilisateur
- Mot de passe
- Certificat électronique
- Numéro de jeton (token)

## 17.5 Mettre à jour les applications régulièrement

---

- Les applications doivent être mises à jour régulièrement pour corriger les vulnérabilités connues.

## 17.6 Sécuriser l'infrastructure

---

- L'infrastructure sur laquelle l'application est exécutée doit être sécurisée. Cela inclut, par exemple, la sécurisation du serveur web, de la base de données et du réseau.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

DOC - Modèle Accord de Confidentialité Fournisseurs

## 17.7 Maitrise des bibliothèques et des Framework

---

- Évaluez l'intérêt de l'ajout de chaque dépendance. Chaque élément rajouté est une augmentation de la surface d'attaque.
- Dans le cas où une seule bibliothèque propose plusieurs fonctionnalités, n'intégrez que les fonctionnalités dont vous avez effectivement besoin.
- Utiliser des Framework et des bibliothèques maintenus, sans vulnérabilités connues.
- Dans le cas d'utilisation de logiciel libre ou open source, les équipes de développement doivent privilégier des projets ou des solutions avec une communauté active, des mises à jour régulières et une bonne documentation.
- Les équipes de développement doivent s'assurer de respecter les règles de licences imposées par les solutions utilisées.

## 17.8 Habilitations

---

- La gestion des habilitations sera prise en compte dans les développements en prévoyant notamment une hiérarchie des droits des utilisateurs afin que chaque personne puisse avoir un accès limité en fonction de ses responsabilités.
- La gestion des profils utilisateurs doit s'accompagner d'un système de journalisation afin de tracer les activités, et détecter toutes anomalies ou événements liés à la sécurité, comme les accès frauduleux et les utilisations abusives de données personnelles.

## 17.9 Gestion des sessions utilisateurs

---

- La gestion des sessions utilisateurs sera prise en compte dans les développements en prévoyants notamment la gestion du délai d'inactivité, la fermeture / déconnexion de la session

## 17.10 Journalisation de l'application et des composants.

---

- L'application doit être développée de manière à fournir des journaux exhaustifs permettant de gérer notamment :
  - Les tentatives de connexion (Succès / Echec)
  - Les tentatives de modification de mot de passe (Succès / Echec)
  - Les modifications de permissions
  - Les modifications d'attributs.
  - Les activités de l'application (Consultation, modification, ...)
  - Les erreurs
  - ...etc.
- Les traces devront être mises à disposition et accessibles gratuitement dans un format lisible, exploitable et interopérable (ATNA : format IHE, syslog, requête dans une base de données à fournir, fichier à décrire), à moins qu'un outil d'analyse soit joint au logiciel.
- Les traces doivent pouvoir être épurées au-delà du temps légal de rétention notamment en conformité avec le RGPD.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

DOC - Modèle Accord de Confidentialité Fournisseurs

- Les équipes de développement prendront un soin particulier à la qualification des remontées d'erreurs dans les journaux (Info, Warn, Err, Debug).

### 17.11 Audits de sécurité

---

- Des audits de sécurité doivent être réalisés régulièrement pour évaluer l'état de sécurité de l'application.
- L'application doit être testée de manière approfondie pour identifier et corriger les vulnérabilités de sécurité.
- Les tests doivent couvrir tous les aspects de l'application, y compris la conception, le code, les données et l'infrastructure.
- Le fournisseur effectuera systématique des tests des applications pour les vulnérabilités connues avant déploiement chez le client
- Le fournisseur devra pouvoir fournir à minima une copie de la synthèse managériale des rapports d'audits de sécurité de l'application sur première demande du GRADeS BFC.

### 17.12 OWASP

---

L'OWASP est une fondation mondiale à but non lucratif qui a pour mission d'améliorer la sécurité des logiciels et des applications web. Elle fournit gratuitement des ressources, des outils et des bonnes pratiques afin d'aider les organisations à développer, acquérir et maintenir des applications sécurisées.

Le OWASP Top 10 est un document de référence international qui recense les dix catégories de vulnérabilités de sécurité les plus critiques pour les applications web, mises à jour régulièrement. Il sert de guide de sensibilisation et de base minimale de bonnes pratiques pour la conception, le développement et l'audit de la sécurité applicative.

- Le fournisseur doit concevoir, développer, intégrer, exploiter et maintenir ses applications et services conformément aux bonnes pratiques de sécurité applicative publiées par l'OWASP (Open Worldwide Application Security Project).
- Les équipes de développements sont sensibilisées au Top 10 des exigences de l'OWASP (dernière version en vigueur)
- Des méthodes de détection des vulnérabilités de code sont mises en place comme une analyse par outil SAST (Static Application Security Testing) par exemple, pour identifier des vulnérabilités potentielles et les corriger.
- Le fournisseur devra être en mesure de démontrer l'analyse et de fournir la liste des écarts avec les justifications associées.

### 17.13 Livraison des développements

---

- Le fournisseur est tenu de livrer des services (applications + composants) exempt de toutes vulnérabilités connues au moment de la livraison au GRADeS BFC.

### 17.14 Données Personnelles

---

- Le développement doit imposer des formats de saisie et d'enregistrement des données qui minimisent les données collectées.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

- Éviter le recours à des zones de texte libre ou de commentaires, sources de collecte de données personnelles supplémentaires non nécessaires ou disproportionnées.

## 18 Exigence spécifique : Sécurité dans les services en nuage

- Les services hébergés devront respecter les exigences de sécurité des réglementations en vigueur.
- Si le fournisseur ou un de ses sous-traitants « héberge » des données de santé (cf sens donné par le Code de la Santé Publique) celui-ci doit être certifié hébergeur de données de santé conformément à l'article L 1111-8 du Code de la Santé Publique.
- Le fournisseur doit fournir une copie de ses certifications HDS et ISO27001.
- Le Prévenir le GRADeS BFC dans un délai de 5 jours ouvrables de tout événement impactant leur(s) certification(s) (audit critique, suspension, retrait).
- Participer alors à une réunion de crise avec le fournisseur afin de définir un plan d'actions en regard de l'évènement.
- Une authentification d'accès doit permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger. Les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification). La confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et de sa saisie.
- Des Mesures doivent être prévues afin de garantir un accès aux données aux seules personnes habilitées selon les besoins du GRADeS BFC.

### 18.1 Transfert de données

---

- Le fournisseur précisera les pays où sont réalisées les hébergements. Si les données ne sont pas hébergées au sein de l'UE ou dans un pays adéquat le fournisseur informe le GRADeS BFC et met en place un mécanisme de sécurité approprié. Il informe le GRADeS BFC des mesures mise en place avec les éléments de preuve.

### 18.2 Réversibilité des données

---

En fin de contrat, le fournisseur s'engage à fournir une copie exploitable des données (bases de données ou fichiers informatiques avec champs délimités et décrits).

Afin de permettre la réalisation de tests de migration, le GRADeS pourra demander de réaliser la fourniture de copies en cours de contrat

Le fournisseur s'engage à détruire les données en fin de contrat après les avoir restituées au GRADeS BFC. Un procès-verbal de destruction sera alors établi et fourni dans un délai maximum de 1 mois après la date de résiliation.

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

DOC - Modèle Accord de Confidentialité Fournisseurs

## Annexe2 : Attestation Suppression Données

Je soussigné(e) **[Nom, prénom]**, en sa qualité de **[.....]** représentant la société **[Nom de la société, Adresse Complète de la société ]**, atteste avoir procédé, en date du **[JJ/MM/AAAA]**, à la suppression **complète, définitive et sécurisée** de toutes les données liées au projet **[Nom du Projet]**.

Cette suppression inclut expressément :

- L'ensemble des fichiers initiaux transférés,
- Toutes copies, sauvegardes, caches, historiques, journaux ou fichiers dérivés,

Je certifie n'avoir conservé **aucune copie résiduelle**, sous quelque forme que ce soit,

Fait pour servir et valoir ce que de droit.

Date :

Nom, fonction et signature du signataire :

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*

## 19 Liens

\*\*\*\*\* Fin du Document \*\*\*\*\*

Seule la version électronique disponible sous le logiciel QSE AVANTEAM de ce document est valide, toute version papier est réputée périmée.

**Attention** : Les zones entourées de crochets [ ] en *italique et bordeaux* et les zones en *italique et bleu* sont des champs automatiques. Merci de ne pas les modifier.

*DOC - Modèle Accord de Confidentialité Fournisseurs*