

CCTP – LIVRET 2

ACCORD-CADRE DSSE-TMA-SIHAM-26-18

Relatif à la tierce maintenance applicative et évolutive de la solution de gestion des ressources humaines Siham (HR Access FPE) des établissements d'enseignement supérieur et de recherche

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES *LIVRET 2*

DESCRIPTION DU CADRE NORMATIF OPERATIONNEL

Objet : Ce livret détaille les différentes exigences opérationnelles (cadre normatif) que devra respecter le candidat pour l'exécution des prestations faisant l'objet du présent accord-cadre.



TABLE DES MATIERES

1. INTRODUCTION	4
2. STANDARDS ET NORMES TRANSVERSES	4
3. EXIGENCES DE SECURITE	5
4. CADRE DE GOUVERNANCE DU PROJET SIHAM	8
4.1. Maîtrise d'œuvre – maîtrise d'ouvrage	8
4.2. Pilotage et coordination interne des prestations à la charge du Titulaire	8
4.3. Gouvernance de la TMAE	8
5. NORMES DE PARAMETRAGE ET DE DEVELOPPEMENT	9
6. STANDARDS ET METHODES DE MAINTENANCE	9
6.1. Maîtrise des périmètres, engagement de résultat	9
6.2. Garantie de fonctionnement de Siham sur l'ensemble des environnements d'exploitation précisés dans le présent CCTP	9
6.3. Modalités de gestion de la configuration	10
6.4. Processus de livraison	10
6.5. Gestion des tests	10
6.5.1. Démarche de test	10
6.5.2. Outil d'industrialisation des tests	11
7. STANDARDS D'ASSISTANCE ET DE DEMANDE DE MAINTENANCE	11
7.1. Définitions	11
7.1.1. Demandes d'assistance	11
7.1.2. Demandes de maintenance	12
7.2. Outillage	12
7.3. Plage d'ouverture du support	13
7.4. Délais de prise en charge et traitement des demandes de maintenance et d'assistance	13
7.4.1. Demandes d'assistance	13
7.4.2. Demandes de maintenance	13
8. STANDARDS EN MATIERE D'ADMINISTRATION ET D'EXPLOITATION DE LA PLATEFORME PROJET	14
9. POLITIQUE ET DEMARCHE QUALITE ET D'AMELIORATION CONTINUE APPLIQUEE A SIHAM	15
9.1. PAQ Siham et PAQ titulaire	15
9.2. PGC Siham et PGCL titulaire	15
9.3. PGD Siham	16
9.4. Amélioration continue	16
10. EXIGENCES DE NIVEAUX DE SERVICE	17
11. ANNEXES	17
11.1. Annexe 1 : Présentation des standards et normes transverses, applicables à l'Amue	17
11.2. Annexe 2 : Sécurité	17



11.3.	Annexe 3 : Normes de paramétrage et développement	17
11.4.	Annexe 4 : Processus de livraison	17
11.5.	Annexe 5 : Outillage d’industrialisation des tests	17
11.6.	Annexe 6 : Présentation de Supcoop	17
11.7.	Annexe 7 : Plan d’assurance qualité Siham	18
11.8.	Annexe 8 : Tableau des exigences de niveau de service	18



1. Introduction

Le présent document constitue le Livret 2 du Cahier des Clauses Techniques Particulières (CCTP) de l'accord-cadre ayant pour objet la tierce maintenance applicative et évolutive de la solution de gestion des ressources humaines Siham (HR Access FPE) des établissements d'enseignement supérieur et de recherche.

Ce livret 2 du CCTP décrit le cadre normatif, les exigences opérationnelles que devra respecter le Titulaire pour l'exécution des différentes prestations attendues au titre du présent accord-cadre. Ce document constitue un socle minimal et met l'accent sur les sujets que l'Amue souhaite porter à l'attention des candidats dans la construction de leur offre.

Ces éléments seront repris et complétés lors de la phase de lancement et d'installation pour constituer le corpus documentaire relatif à la qualité et à la sécurité du projet et des prestations de TMAE : PAQ, PAS, PGD, PGCL...

Une fois constitués et validés par l'Amue, ces documents auront valeur contractuelle (cf. CCAP) pour l'évaluation de la qualité et la réception des prestations.

Le livret 2 du CCTP s'articule autour de la présentation :

- Des standards et normes transverses ;
- Des exigences de sécurité ;
- Du cadre de gouvernance du projet Siham ;
- Des normes de paramétrage et de développement ;
- Des standards et méthodes de maintenance ;
- Des standards d'assistance et de demande de maintenance ;
- Des standards en matière d'administration et d'exploitation de la plateforme projet ;
- De la politique et démarche qualité et d'amélioration continue appliquée à Siham ;
- Des exigences de niveaux de service.

2. Standards et normes transverses

Dans le cadre de la politique de modernisation de l'action publique, les établissements publics de l'Etat doivent se conformer aux standards et normes construits et maintenus par les différents services de l'Etat : Direction Interministérielle de la Transformation Publique (DITP) et Direction Interministérielle du Numérique (DINUM), Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)...

Ces standards et normes ont pour objectif d'accroître la cohérence des systèmes d'information conçus, développés et maintenus par les services centraux et déconcentrés de l'État, collectivités publiques, éditeurs de logiciel, prestataires de services, etc.

Le détail de ces standards et normes transverses à l'Amue est présenté en annexe 1 du présent livret.

Ces standards et normes transverses sont donc applicables à l'ensemble des produits développés et maintenus par l'Amue, dont ceux faisant l'objet du présent accord-cadre (Siham et ses solutions associées).

L'ensemble des travaux, et en particulier les évolutions fonctionnelles et techniques, mis en œuvre par le Titulaire au titre du présent accord-cadre, doivent s'inscrire, sauf décision contraire partagée par l'Amue et le Titulaire, dans le cadre de ces standards et normes.

L'Amue attire l'attention du Titulaire sur le fait, qu'au titre de la maîtrise d'œuvre de l'ensemble des postes, il est garant du respect des standards et normes.



3. Exigences de sécurité

La sécurité constitue un enjeu fort pour l'Amue et pour le projet Siham.

Il s'agit pour l'Amue de respecter les obligations et recommandations qui lui sont dictées en matière de sécurité des SI en tant qu'opérateur de l'Etat, mais aussi de maintenir sur le long terme la confiance des de l'Amue lorsque ceux-ci déploient et utilisent ses solutions, dont Siham. Il s'agit également pour la TMAE de respecter la politique de sécurité de l'Amue.

Le Titulaire doit se conformer aux documents et aux exigences suivantes, ainsi qu'à l'ensemble des standards et normes identifiées ou décrites dans les annexes :

- Objectifs de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 ([Politique de sécurité des systèmes d'information de l'Etat - Légifrance \(legifrance.gouv.fr\)](https://www.legifrance.gouv.fr/eli/circulaire/2014/07/17/5725/SG)) ;
- Les recommandations de l'ANSSI ;
- Le Référentiel Général de Sécurité (RGS) :
<https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/referentiel-general-de-securite/>
- La politique de gestion des comptes et des mots de passe de l'Amue ;
- Le Plan d'assurance Sécurité, reprenant les exigences ci-dessous :
 - Sélection des composants technique au regard des vulnérabilités existantes ;
 - Utilisation de jeux de données non extraits de la production ou anonymisés ;
 - Aucun accès direct depuis internet aux serveurs applicatifs des plateformes projet AMUE, obligation de passer par un VPN ;
 - Utilisation de systèmes d'Authentification et de contrôle d'accès de confiance ;
 - Respect du Top 10 OWASP dans les développements ;
 - Respect du droit d'audit de l'AMUE ;
 - Prendre en compte la sécurisation des configurations par défaut des plateformes projet ;
 - Devoir de réserve et astreintes au secret professionnel ;
 - Description de la prise en charge de la sécurité au niveau de l'organisation et du marché ;
 - Description de la fréquence et du contenu des formations et sensibilisations ;
 - Le Titulaire dispose d'un site sûr ;
 - Présence de dispositifs et de moyens pour protéger les actifs de l'AMUE (antivirus, protection du réseau contre les compromissions) ;
 - Présence d'une politique, de mesures et de dispositifs pour gérer le contrôle d'accès à ses locaux et à ses systèmes d'information ;
 - Présence de procédures de gestion interne des vulnérabilités de sécurité sur le système d'information ;
 - Présence de procédures de gestion des incidents internes de sécurité sur le système d'information ;
 - Présence de moyens de contrôle pour s'assurer du respect des exigences de sécurité de l'AMUE par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre des prestations ;
 - Accompagnement obligatoire par du personnel AMUE sur les sites de l'AMUE. Interdiction d'utiliser du matériel numérique d'enregistrement de toute nature dans les locaux de l'AMUE sans son accord ;
 - Mise en œuvre de moyens techniques afin de protéger de toutes divulgations indésirables volontaires ou accidentelles, les informations relatives à l'AMUE (lors du stockage ou des échanges). Effacement des informations à la demande ou en fin de marché après rétrocessions des informations ;
 - Présences de mesures et dispositifs garantissant le retour à l'AMUE et la destruction des informations de l'AMUE à l'expiration ou à la résiliation du marché ;



- Présence d'un registre de traitement consultable à tout moment par l'AMUE ou la CNIL ;
- Présence d'un processus de gestion des incidents de sécurité liés à l'application Siham (impact de l'incident en termes de nombres d'utilisateurs et de quantité de données exposées, proposition de contre-mesures, proposition de correctifs) ;
- Présentation des outils et méthodes mis en œuvre pour atteindre l'objectif de conformité ;
- Le titulaire doit porter une attention particulière au cadre réglementaire applicable en termes de SSI ;
- D'un point de vue technique, il est requis de la part du titulaire d'appliquer les différents guides de l'ANSSI ;
- Le Titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. L'Amue est autorisée à vérifier, conformément à la clause d'audit, la réalité de cet engagement ;
- L'aide du Titulaire peut être requise pour évaluer l'impact d'un incident de sécurité sur les DCP en nombre d'utilisateurs et en quantité de données exposées ;
- L'aide du Titulaire peut être requise pour fournir les correctifs nécessaires à la résolution de l'incident ;
- En cas d'incident de sécurité touchant le SI du Titulaire et pouvant mettre en péril les DCP confiées par l'AMUE (notamment, compromettant les accès au SI AMUE utilisés pour la réalisation des prestations), le titulaire informe immédiatement et de manière exhaustive l'AMUE de l'événement.

En ce qui concerne la formation de ses équipes y compris sous-traitants, le titulaire forme et sensibilise son personnel intervenant dans le cadre des prestations à la sécurité de l'information, à la sécurité du numérique, à la protection des données à caractère personnel et aux règles de l'Amue. À ce titre, il fournit à l'Amue les programmes et attestation de formation et de sensibilisation de ses personnels.

En l'absence de programme dédié en interne, le titulaire se base sur les MOOC « Atelier RGPD » de la CNIL et « SecNumacademie » de l'ANSSI pour la formation et fournit les certificats de réussite de ces MOOC à l'Amue. Le titulaire veille notamment à ce que son personnel intervenant pour l'exécution des prestations respecte les dispositions du présent accord-cadre concernant la sécurité et la protection des données personnelles.

Ce *Plan d'Assurance Sécurité* sera mis au point lors de la phase de lancement et d'installation et mis à jour tout au long de l'accord cadre au titre des travaux de maîtrise d'œuvre d'ensemble.

Un modèle de PAS, une présentation des exigences minimum de sécurité à remplir par le prestataire et la politique de gestion des comptes et mot de passe sont disponibles en annexe du CCTP.

a. La localisation des données, un enjeu stratégique

Choisir le lieu d'hébergement et de stockage de ses données et garantir que celles-ci sont stockées sur le territoire de l'Union européenne est devenu dans le cadre du RGPD une véritable exigence pour la stratégie de gestion des risques de toute entreprise.

Les moyens utilisés pour exécuter les prestations nécessitant un accès aux données de production des établissements et de l'Amue, doivent être localisés sur le territoire des Etats membres de l'Union européenne.

Dans le cadre de l'accord-cadre de TMAE Siham, pour les prestations de type assistance aux établissements ou administration de plateforme, un accès aux données réelles de production (données à caractère personnel du domaine RH) pourrait être nécessaire à la réalisation de la prestation.

Les marchés subséquents et/ou les bons de commande préciseront les exigences en matière de localisation des données et des équipes effectuant les traitements.



b. Protection des flux d'échange de données

Tous les échanges d'information avec les différents acteurs interagissant avec Siham doivent être protégés en intégrité et en confidentialité par l'intermédiaire de canaux sécurisés. Cette exigence doit être déclinée par le titulaire en fonction des spécificités de chacun des environnements constituant la solution Siham :

- Les connexions de l'ensemble des personnels du Titulaire doivent s'effectuer au travers d'un ou plusieurs VPN site à site ;
- L'extrémité du VPN côté Titulaire doit être un équipement géré sous sa responsabilité. Ce point permet de garantir à l'Amue que les postes autorisés à se connecter à cet équipement et à emprunter le VPN jusqu'à l'Amue respecteront une politique de sécurité validée par le Titulaire et conforme au marché Siham ;
- Le Titulaire s'engage à identifier et authentifier individuellement toute personne accédant au SI de l'Amue au travers du VPN, limitant cet accès à la liste des personnes intervenant sur la TMAE Siham et fournie à l'Amue dès qu'intervient une arrivée ou un départ de personnel. Ce point est indispensable dans la mesure où l'Amue s'interconnecte avec un site extérieur acceptant de fait de ne plus maîtriser l'identification et l'authentification de chaque utilisateur ;
- Concernant l'identification des postes de travail des personnels, le Titulaire fournit à l'Amue la ou les plages d'adresses IP utilisées ;
- Le VPN site à site doit utiliser la technologie IPsec ;
- Les caractéristiques techniques du VPN IPsec mis en œuvre doit respecter les recommandations de l'ANSSI ;
- Le Titulaire accepte de se conformer aux règles de filtrage mises en œuvre par l'Amue à l'entrée de la plateforme projet.

c. Protection des informations sensibles

Toute opération de destruction d'information ou de données sensibles doit être assurée de façon sûre. Les documents doivent être détruits avec les moyens appropriés. Les supports de stockage physiques n'ayant plus d'utilité opérationnelle dans leur contexte d'emploi initial doivent être effacés de manière sûre avant leur mise au rebut ou leur réutilisation.

Pour respecter les obligations de protection des données à caractère personnel exprimées par la Commission Nationale de l'Informatique et des Libertés, chaque donnée doit être protégée contre tout risque d'accès non autorisé, ou intrusion, au sein même de l'infrastructure supportant les services de Siham et quels que soient les traitements mis en œuvre, y compris vis-à-vis des acteurs internes opérants sur cette infrastructure. En d'autres termes, à l'intérieur même de l'espace de confiance du système Siham, un « périmètre » ayant un niveau de protection renforcé doit être établi.

d. Une organisation globale de la gestion des risques SSI

La mise en place d'une organisation transverse et globale pour le management des risques SSI pour l'ensemble du projet Siham est indispensable pour assurer une maîtrise satisfaisante de la confidentialité et de la sécurité des données sensibles qui sont manipulées par la solution Siham.

Cette organisation offre l'opportunité de planifier, de mettre en œuvre, de vérifier et d'améliorer le niveau de confiance dans Siham pendant toute la durée de vie de la solution.

L'instauration d'un Comité de Gestion des Risques SSI dédié au projet avec une organisation des activités afférentes est une première réponse apportée à cet objectif.



4. Cadre de gouvernance du projet Siham

4.1. Maîtrise d'œuvre – maîtrise d'ouvrage

Dans le dispositif contractuel de la TMAE Siham, la répartition des rôles et responsabilités entre l'Amue et le Titulaire de l'accord cadre est la suivante :

	Accord Cadre	Marché Subséquent Amue	Marché Subséquent Etablissement
Acheteur	Amue	Amue	Etablissement à l'origine du marché subséquent
Représentant de l'acheteur	Le directeur de l'Amue	Le directeur de l'Amue	Le président / directeur de l'Etablissement ou son représentant
Maîtrise d'ouvrage (MOA)	Amue Représenté par la direction projet Siham		L'Etablissement Un interlocuteur privilégié sera désigné à l'occasion de la contractualisation du marché subséquent
Maîtrise d'œuvre (MOE)	Titulaire		

4.2. Pilotage et coordination interne des prestations à la charge du Titulaire

Le Titulaire est le maître d'œuvre des postes de la TMAE qui lui sont confiés.

Au titre de la prestation de « maîtrise d'œuvre d'ensemble » de chacun des postes, le Titulaire exerce une maîtrise d'œuvre globale et transverse en matière de pilotage et de coordination de l'ensemble des activités conduites au titre du présent accord-cadre.

En particulier, il est attendu du Titulaire qu'il mette en place un dispositif de pilotage et de coordination le plus intégré possible, regroupant, à minima, les opérations relatives à chacune des grandes familles de postes de prestation :

- Maintenance évolutive ;
- Maintenance corrective et adaptative, couvrant l'ensemble de la chaîne de maintenance incluant l'administration et l'exploitation de la plateforme projet ;
- Support et assistance aux établissements en exploitation ;
- Déploiement et diffusion.

L'organisation et le dispositif de pilotage internes du Titulaire doivent être décrits dans son offre et s'inscrire dans l'engagement relatif aux activités de Maîtrise d'œuvre d'ensemble applicable à l'ensemble des postes de prestations. Ils pourront être précisés lors de la phase de lancement et d'installation et mis à jour, si nécessaire, pendant la durée d'exécution de l'accord-cadre.

Il est attendu que le Titulaire propose des méthodes et des outils de planification et coordination de son équipe et de reporting afin d'alimenter les instances de gouvernance de la TMAE, et de piloter l'avancement des travaux des postes en cohérence avec le plan projet Siham.

L'ensemble de ces dispositions doit être conforme aux règles de qualité, de sécurité et de confidentialité applicables à l'accord-cadre.

4.3. Gouvernance de la TMAE

La description de la gouvernance du projet Siham et le rôle attendu du Titulaire sont présentés dans le livret 1 du CCTP.



5. Normes de paramétrage et de développement

Les équipes du titulaire s'engagent à suivre les normes et standards de développements (**NSD**) définis sur le projet. Ces normes sont référencées dans un document qui est maintenu dans le cadre des prestations de maintenance de la solution Siham.

Le document actuellement en vigueur sur le projet est le document *SIHAM_PAQ_QUA_NormesEtStandDev(2.00)*, en annexe 3 de ce livret.

Ce document est revu, complété et pris en compte pour application lors de la phase de montée en compétences du nouveau titulaire en charge de la maintenance du produit.

6. Standards et méthodes de maintenance

6.1. Maîtrise des périmètres, engagement de résultat

En tant que maître d'œuvre, intégrateur de Siham, le Titulaire est responsable des choix de conception technique et d'implémentation à l'état de l'art.

Cette responsabilité implique, pour les prestations sur devis, un engagement de résultat pour un prix fixe défini.

Dans le cadre d'une maintenance – fonctionnelle ou technique – évolutive, corrective ou préventive, en cas d'un défaut d'analyse de la complexité des évolutions (respectivement corrections) à réaliser ou d'une erreur ou d'un oubli de conception pouvant induire, pendant ou après le développement de la solution, un retour en conception et une reprise des développements déjà réalisés, le Titulaire s'engage – en dehors de la phase de lancement et installation - à traiter la reprise de l'analyse et de la conception sans surcoût pour l'Amue.

En revanche, pour tout changement dans l'expression des besoins fonctionnels, des exigences fonctionnelles ou non fonctionnelles induites par des critères de qualité logicielle, l'Amue s'engage à prendre à sa charge les coûts d'adaptation induits, sur la base de devis détaillés indiquant clairement l'analyse des surcoûts par rapport à la phase de construction en cours et aux éléments logiciels et documentaires impactés.

En tant que propriétaire de la solution Siham, l'Amue peut exprimer son désaccord sur des orientations proposées par le Titulaire et indiquer des orientations qui lui semblent préférables, notamment si elles sont préconisées par l'éditeur. À tout moment, le Titulaire, exerçant son devoir de conseil, doit exprimer ses arguments pour justifier ses propositions et préconisations. Dans le cas, où l'Amue imposerait une solution au Titulaire et si celui-ci n'a pas détaillé par écrit ses arguments étayés par une analyse des risques et des impacts, il resterait pleinement responsable de la mise en œuvre. Dans tous les cas, le Titulaire est responsable des défauts d'implémentation.

6.2. Garantie de fonctionnement de Siham sur l'ensemble des environnements d'exploitation précisés dans le présent CCTP

Dans le cadre du présent accord-cadre, il appartient au Titulaire, dans le respect du PAQ, de :

- Maintenir les normes de paramétrage et de développement qui, une fois validées par l'Amue, garantissent une conformité du maintien en conditions opérationnelles et des maintenances fonctionnelle ou technique des produits entrant dans le périmètre du présent accord-cadre ;
- Mettre en œuvre les dispositifs de production conformes à ces normes ;
- L'Amue mettra à disposition du Titulaire les matériels et logiciels de base lui permettant de conduire l'ensemble des tests nécessaires pour vérifier le fonctionnement de chaque livraison sur une plateforme représentative.



6.3. Modalités de gestion de la configuration

Les modalités de gestion de la configuration des environnements de la plateforme projet sont décrits dans le PGCL et son annexe, fournis en annexe du livret 1 du présent CCTP.

En tant que maître d'œuvre, l'intégrateur est responsable du respect du PGCL édicté et peut fournir des compléments et ou modifications au PGCL en vigueur.

Le respect du PGCL permet d'assurer sur l'ensemble de la plateforme projet l'unicité des éléments constitutifs de la solution Siham et sa traçabilité dans le cadre des actions de TMAE. Les différents acteurs doivent donc se conformer aux règles définies et fournir régulièrement les informations nécessaires au suivi des modifications apportées.

6.4. Processus de livraison

Les processus de livraison sont décrits dans le PGCL et fournis en annexe 4 de ce présent livret.

Le Titulaire est tenu d'en respecter les différentes modalités et de les maintenir à jour en fonction de l'évolution du contexte.

Le Titulaire a également la charge de proposer des compléments et des ajustements dans un objectif d'amélioration continue.

6.5. Gestion des tests

6.5.1. Démarche de test

Les deux typologies de tests attendus (tests fonctionnels et non fonctionnels) sont regroupées dans les tests d'intégration/validation puis dans les tests de non-régression. Ils seront détaillés dans le document de stratégie de test. Ci-après une liste non exhaustive des différentes familles de tests.

Les tests fonctionnels

Ils visent à observer le comportement de la solution vis-à-vis des attentes des utilisateurs. L'objectif est de comparer chacune des fonctionnalités en fonctionnement avec les spécifications indiquées dans le cahier des charges.

Les tests non fonctionnels

- **Les tests de montée en charge**
Ils permettent d'évaluer la capacité à supporter de plus en plus d'utilisateurs tout en maintenant une utilisabilité optimale et un fonctionnement correspondant aux cahiers des charges.
- **Les tests de robustesse**
La solution est soumise à une forte activité, afin de vérifier si le fonctionnement est optimal avec une charge importante. Ils permettent aussi de vérifier le bon fonctionnement si l'environnement est altéré (réseau LAN, WAN, ...)
- **Les tests aux limites**
De la même manière que les tests de robustesse, ils permettent de vérifier si le fonctionnement reste en adéquation avec le plus grand nombre d'utilisateurs possible ayant un accès simultané à la solution durant de forte sollicitation des plateformes selon les usages de la solution.
- **Les tests de performance**
L'objectif est de simuler la disponibilité de la plateforme technique lors du fonctionnement du logiciel : consommation CPU, utilisation de la mémoire vive, volume de commandes lancées à la seconde ou encore le mouvement d'entrée et de sortie des utilisateurs.
- **Les tests de compatibilité de plateforme**
Ces tests permettent de vérifier le bon fonctionnement de la solution sur des environnements similaires aux plateformes des centres de production des utilisateurs.
- **Les tests d'ergonomie**



L'objectif est d'anticiper l'expérience utilisateur dans le cadre de la norme RGAA (sentiment de l'utilisateur à travers l'interface de la solution) : Design global, cinématique applicative, analyse de la gestuelle utilisateur,

- **Les tests d'interface graphique**

L'objectif est de s'assurer que la présentation graphique est suffisamment attrayante pour être acceptée par les utilisateurs et qu'elle réponde aux normes RGAA.

- **Les tests de sécurité**

L'objectif est de valider si les niveaux de sécurité spécifiés dans les normes et études sont implémentés et fonctionnels.

Une présentation de la démarche de recette et de test est fournie dans le Plan assurance Qualité du projet SIHAM en annexe 7 du présent livret.

6.5.2. Outil d'industrialisation des tests

Dans une démarche d'industrialisation, de sécurisation et d'amélioration de la qualité des différentes phases de tests (cf. supra), l'Amue a retenu un outillage, Squash TM.

Une présentation de cet outil est fournie en annexe 5 du présent livret.

Le Titulaire est tenu d'intégrer pleinement cet outillage, fourni par l'Amue, dans sa démarche.

7. Standards d'assistance et de demande de maintenance

Les standards d'assistance et de demande de maintenance applicables au Titulaire du présent accord cadre s'inscrivent dans le cadre des engagements que prend l'Amue en matière de support qu'elle propose aux établissements Siham.

En effet, pour rappel, le support utilisateur de premier niveau est pris en charge et est de la responsabilité des établissements. Les incidents ou les demandes d'assistance non résolus sont escaladés par les correspondants Siham en établissement aux équipes de l'Amue.

Après qualification, une partie de ces demandes d'assistance et de maintenance sont externalisées au Titulaire de l'accord-cadre.

7.1. Définitions

On distingue principalement :

- Les demandes d'assistance (et demandes d'informations)
- Les demandes de maintenance

7.1.1. Demandes d'assistance

Les demandes d'assistance regroupent l'ensemble des sollicitations formulées par les établissements. A la suite de sa qualification par l'Amue, une demande d'assistance peut être qualifiée en demande de maintenance (cf. §7.1.2).

On distingue trois niveaux de criticité des demandes d'assistance :

- Demande d'assistance **Bloquante**

Une demande est classifiée Bloquante si le nombre d'utilisateurs concernés ou si l'impact sur le résultat des activités sont potentiellement élevés. Les demandes d'assistance incluent les incidents de fonctionnement de la solution correspondant soit à une interruption imprévue d'un service SI ou chaque fois qu'un événement détériore ou perturbe fortement le niveau de service.

L'Amue peut déclasser une demande Bloquante en demande Majeure ou Mineure si les éléments d'information qui sont fournis ne permettent pas de reconnaître les critères définis ci-avant ou si,



lors des échanges avec l'établissement, celui-ci réagit dans des délais incompatibles avec une demande bloquante. Par défaut, toute réponse attendue de l'établissement effectuée dans un délai de plus d'1 jour ouvré induit une déclassification en Non Bloquante à savoir Majeure ou Mineure.

- Demande d'assistance **Majeure**

Est ainsi classifiée, toute demande qui ne répond pas aux critères de classification d'une demande Bloquante. Une demande d'assistance **Majeure** permet la production d'un résultat conforme même si l'utilisation n'est pas optimale, par l'usage par exemple d'une solution de contournement.

- Demande d'assistance **Mineure**

Est une demande qui n'est ni bloquante, ni majeure.

7.1.2. Demandes de maintenance

Une demande de maintenance correspond soit :

- À un *dysfonctionnement* détecté dans l'utilisation du système en exploitation,
- Au *non-respect des spécifications* de la solution,
- L'expression d'un *nouveau besoin*.

Une demande de maintenance peut porter sur la solution logicielle Siham, les interfaces, mais aussi sur la documentation, les outils de déploiement / diffusion (kits) ou encore les traitements de remise en qualité des données.

On identifie 3 niveaux de criticité des demandes de maintenance :

- Demande de maintenance **Bloquante**

Une demande de maintenance Bloquante est relative à un événement survenu qui affecte la disponibilité ou l'utilisabilité d'un service, la conformité des résultats vis-à-vis des règles métiers, sa sûreté de fonctionnement comme l'intégrité ou la confidentialité des données. Une demande de maintenance bloquante induit la livraison rapide d'une solution au regard de l'explicitation des impacts.

- Demande de maintenance **Majeure**

Une demande de maintenance Majeure est une demande relative à un événement qui n'est pas considéré comme bloquant même s'il affecte l'utilisabilité optimale d'un service sans toutefois empêcher la production d'un résultat conforme.

Elle peut correspondre également à la signalisation d'un risque comme une faille de sécurité ou un événement à venir préjudiciable à la disponibilité du service, à la qualité de ses résultats et à sa sûreté de fonctionnement.

Enfin une demande de maintenance peut correspondre à l'expression d'un nouveau besoin impliquant d'étendre le périmètre fonctionnel ou technique du système, sans qu'il soit relatif à la correction d'un problème avéré. Dans ce cas elle est définie comme une demande majeure, ou une demande mineure en fonction de la valeur ajoutée attendue pour la communauté d'utilisateurs.

- Demande de maintenance **Mineure**

Est une demande qui n'est ni bloquante, ni majeure.

7.2. Outillage

L'outil de gestion et de suivi des demandes de maintenance et d'assistance, de la prise en charge, jusqu'à la résolution définitive est fourni par l'Amue et doit être impérativement utilisé par le Titulaire.

L'outil utilisé dans le cadre de ce nouveau marché est l'outil SUPCOOP, SUPport COOpératif, adossé à la solution JIRA. Une présentation de SUPCOOP est fournie en annexe 6 du présent livret.



7.3. Plage d'ouverture du support

Le Titulaire doit être en mesure d'assurer la prise en charge et le traitement des demandes de maintenance et d'assistance :

- Tous les jours ouvrés (du lundi au vendredi, hors jours fériés) ;
- De 8h à 18h.

7.4. Délais de prise en charge et traitement des demandes de maintenance et d'assistance

7.4.1. Demandes d'assistance

Le Titulaire doit satisfaire les délais de traitement des demandes d'assistance suivants :

Criticité	Délai de réponse
Bloquant	≤ 1 Jours ouvrés
Non bloquant (majeure/mineure)	≤ 3 Jours ouvrés

Précisions :

- Les délais sont décomptés à partir de la date de transmission (affectation) de la demande au Titulaire et sur la base des plages de service du support.
- Le non-respect de ses niveaux de service peut donner lieu à l'application de pénalités.

7.4.2. Demandes de maintenance

Le Titulaire doit satisfaire les délais de résolution des demandes de maintenance suivants :

Criticité	Délai de réponse avec une solution de contournement ou une correction pérenne	Délai de correction pérenne si solution de contournement identifiée au préalable	
Bloquante	≤ 2 Jours ouvrés	Si solution contournement induit une forte dégradation du service	≤ 7 Jours ouvrés pour un niveau de service correct
		Si solution contournement induit un niveau de service correct	Livraison dans un prochain lot de diffusion
Majeure	≤ 10 Jours ouvrés	Livraison dans un prochain lot de diffusion	
Mineure	Lot de diffusion ET / OU Remis à arbitrage budgétaire	N/A	

Précisions :

- Les délais sont décomptés à partir de la date de transmission (affectation) de la demande au Titulaire et sur la base des plages de service du support.
- Le non-respect de ses niveaux de service peut donner lieu à l'application de pénalités.



8. Standards en matière d'administration et d'exploitation de la plateforme projet

Il est attendu du Titulaire au titre du présent accord cadre des activités d'administration et d'exploitation de la plateforme projet des solutions rentrant dans le périmètre de maintenance Siham.

A ce titre, Le Titulaire proposera une organisation en conséquence et nommera un responsable technique pour les aspects architecture de la solution et un responsable d'exploitation de la plateforme projet.

Le Titulaire doit respecter les exigences de niveaux de service en matière de disponibilité de la plateforme projet et d'intégrité applicatives tels que définis dans le CCAP, **sur la plage de service de 8h à 18h** (hors week-end et jours fériés). En conséquence, les opérations de maintenance ayant un impact sur la disponibilité de la plateforme sont, sauf autorisation de l'Acheteur, à effectuer en dehors de cette place de service.

La plateforme projet Siham est entièrement réinternalisée et hébergée au sein d'une infrastructure de l'ESR (UNISTRA et UB). La mise à disposition des ressources d'infrastructure, telles que décrites dans le livret 1 du CCTP, est pilotée par l'Amue en coordination avec le Titulaire du présent accord-cadre.

Pour l'ensemble des composants et services s'exécutant sur la plateforme projet, l'Amue fixe la feuille de route et fournit au Titulaire les licences nécessaires. Il peut toutefois déléguer au Titulaire la relation avec les éditeurs dans le cas de demandes de support. Cet accès doit être restreint au périmètre du présent CCTP.

Il s'agit pour le Titulaire de garantir, dans le périmètre des prestations qui lui ont été commandées, l'accès, la disponibilité, la cohérence et l'utilisation de la plateforme projet, par la mise en œuvre, de manière conforme aux exigences du présent accord-cadre, de services d'exploitation et d'administration des environnements de Siham et des éventuelles autres solutions associées.

Ces prestations couvrent à la fois les couches basses et les couches applicatives de la plateforme projet, mais également l'interconnexion réseau entre les locaux du Titulaire et les locaux de l'Amue.

Dans le cadre de ces travaux, le Titulaire veille au respect des exigences de sécurité applicables à cette plateforme (cf. chapitre 3 du présent livret).

En particulier, les exigences attendues relatives à la sécurité des connexions réseaux du Titulaire à la plateforme projet sont les suivantes :

- Les connexions de l'ensemble des personnels du Titulaire doivent s'effectuer au travers d'un VPN site à site ;
- L'extrémité du VPN côté Titulaire doit être un équipement géré sous sa responsabilité. Ce point permet de garantir à l'Amue que les postes autorisés à se connecter à cet équipement et à emprunter le VPN jusqu'à l'Amue respecteront une politique de sécurité validée par le Titulaire et conforme à l'accord-cadre ;
- Le Titulaire s'engage à identifier et authentifier individuellement toute personne accédant au SI de l'Amue au travers du VPN, limitant cet accès à la liste des personnes intervenant sur le projet Siham et fournie à l'Amue dès qu'intervient une arrivée ou un départ de personnel ;
- Concernant l'identification des postes de travail des personnels, le Titulaire fournit à l'Amue la ou les plages d'adresses IP utilisées ;
- Le VPN site à site doit utiliser la technologie IPsec ;
- Les caractéristiques techniques du VPN IPsec mis en œuvre doit respecter les recommandations de l'ANSSI ;



- Le Titulaire accepte de se conformer aux règles de filtrage mises en œuvre par l'Amue à l'entrée de la plateforme projet.

La répartition des responsabilités entre l'Amue et le Titulaire en matière d'administration et d'exploitation des différents composants techniques / services est fournie dans le livret 3 du CCTP. La description des plateformes est fournie dans le livret 1 du CCTP.

9. Politique et démarche qualité et d'amélioration continue appliquée à Siham

L'Amue entend bénéficier de l'apport professionnel, méthodologique et qualité du Titulaire, dans son domaine d'intervention.

La mise en place d'un dispositif qualité opérationnel est indispensable pour assurer la maîtrise et l'efficacité des activités dans lesquelles le titulaire est engagé.

La documentation qualité fournie par le titulaire lors de la phase de lancement à savoir, PAQ, PGCL, Stratégie de tests, Dossier de pilotage et d'organisation doit être mis à jour régulièrement tout au long de l'exécution de l'accord cadre. Ces travaux font pleinement partie des activités de maîtrise d'œuvre d'ensemble compris dans tous les postes de prestations de l'accord-cadre.

Il est de la responsabilité du Titulaire de veiller à ce que tous ses membres et intervenants appliquent les différents documents qualité de référence.

L'Amue tient à souligner l'importance de l'application par toute l'équipe du Titulaire, des processus définis sur le projet en termes de **gestion des configurations logicielles et documentaires**.

9.1. PAQ Siham et PAQ titulaire

Est annexé au présent livret le Plan d'Assurance Qualité (PAQ) Siham (cf. annexe 7). Il est maintenu par le correspondant qualité du projet Siham. Il sera complété lors de la phase de lancement du présent accord-cadre, pour prendre en compte et/ou référencer les documents, dispositifs qualité du titulaire détaillés dans le PAQ du titulaire et validé par l'Amue.

Le Plan d'Assurance Qualité (PAQ) titulaire est l'engagement de celui-ci quant à la politique d'assurance qualité applicable aux prestations. Il s'applique depuis le démarrage du contrat jusqu'à sa clôture, pour garantir la conformité des produits livrés avec les exigences spécifiées dans le cadre de la réalisation du projet. Il est également utilisé pour apporter la visibilité à l'Amue sur l'organisation mise en œuvre pour réaliser les prestations et sur les méthodes appliquées pour obtenir le niveau de qualité répondant aux exigences contractuelles. Il rappelle également les éventuelles obligations de l'AMUE envers le titulaire sur ce contrat. Ce document est à consulter par chaque membre de l'équipe du prestataire en tant que document à mettre en application.

9.2. PGC Siham et PGCL titulaire

Le PGC Siham annexé au livret 1 présente à la fois les éléments d'architecture et de gestion de configuration du projet Siham. Il présente les différents sous-systèmes de la solution avec les éléments d'architecture et activités de gestion de configuration pour chacun d'eux.

Ce document est le point d'entrée du PGCL du titulaire attendu dans le cadre du présent marché. Ce dernier ce devant de détailler les dispositifs de gestion de configuration logicielle sur lesquels le titulaire est engagé pour assurer la qualité de cette gestion permettant une maintenance et des livraisons logicielles conformes.

Siham constitue une souche commune à l'ensemble des Etablissements qui déploient et exploitent la solution chacun au sein de leur Système d'Information, apportant, dans certaines limites, des personnalisations.



Du point de vue des Etablissements, la souche Siham est construite et maintenue « en central » par l'Amue avec comme objectif de ne jamais écraser les paramétrages personnalisés ou les développements effectués par les Etablissements. Le Titulaire doit donc veiller à mettre en place un système de gestion de configuration logicielle (procédures et outillage) permettant de gérer les versions du paramétrage souche, de livrer et installer celui-ci dans le SI des Etablissements. Il doit intégrer également dans son processus de test, des tests de vérification du respect de l'intégrité des paramétrages et développements de personnalisation, notamment lors d'une étape de recette d'installation du paquetage de livraison.

Le PAQ du titulaire doit donc être accompagné d'un PGCL (Plan de Gestion des Configurations Logicielles), auquel l'ensemble des équipes doit avoir été formé et qu'elles doivent appliquer de manière stricte. Ce PGCL devra décrire notamment tous les types de composants logiciels gérés en configuration, les procédures et outillages assurant la qualité en termes de gestion des développements et des livraisons.

9.3. PGD Siham

Le PAQ Siham est accompagné d'un Plan de gestion documentaire (PGD), le titulaire devra se conformer aux processus de gestion documentaires décrits dans ce PGD fourni en annexe 7 de ce livret.

Ce PGD est maintenu par le correspondant qualité du projet Siham. Dans le référentiel qualité sont également mis à disposition des équipes, de nombreux modèles de documents intégrant des guides rédactionnels précisant l'attendu de chaque chapitre.

Ce PGD décrit les processus de gestion de la documentation et définit les règles de nommage et de gestion des versions à respecter.

9.4. Amélioration continue

Au-delà de la bonne exécution des prestations conformes aux besoins et exigences fixées, ainsi que, dans le respect des règles de l'art, il est attendu du Titulaire qu'il soit force de conseil et qu'il mette en place les dispositifs et moyens pour :

- Garantir la qualité de la solution Siham, à l'état de l'art ;
- Anticiper et prévenir les incidents et problèmes ;
- Être force de proposition en cas de survenance d'un incident ou problème pour résoudre le problème dans les délais les plus courts et pour éviter la récurrence de ce problème ;
- Améliorer, en collaboration avec le pouvoir adjudicateur, de manière continue l'organisation et les processus afin de :
 - Renforcer la qualité des services rendus ;
 - Raccourcir les délais d'exécution des travaux ;
 - Maîtriser et diminuer les coûts pour le pouvoir adjudicateur.

Dans cette optique, il est attendu pour le présent accord-cadre de mettre en place une démarche d'amélioration continue, dispositif au travers duquel l'Amue et le Titulaire collaborent pour :

- Définir des axes et des objectifs d'amélioration ;
- Etablir des plans d'actions (court, moyen, long terme), intégrant les moyens mis en œuvre, les conditions de réussites, les contraintes et les acteurs concernés ;
- Définir la répartition des bénéfices des gains obtenus.

A ce stade, quelques axes d'amélioration projet ont d'ores et déjà été identifiés :

- La disponibilité de la plate-forme projet ;
- La mise en place d'une chaîne d'intégration continue, ayant pour objectif une plus grande souplesse et réactivité dans la livraison des évolutions et correctifs ;
- La fiabilité des plannings/jalons, en particulier les jalons de livraison des évolutions et des versions ;



- La réactivité dans la prise en compte des besoins et demandes de l'Amue et des Etablissements ;
- L'efficacité des mécanismes de détermination des charges et des délais ;
- La maîtrise et la sécurisation de la gestion des configurations logicielles ;
- La fiabilisation et l'industrialisation des processus de tests et leurs communications à l'Amue ;
- L'amélioration de la qualité des évolutions mises en œuvre, caractérisée, notamment, par la diminution du taux d'anomalies et du nombre de sollicitation du support ;
- L'optimisation des coûts de maintenance corrective.

10. Exigences de niveaux de service

Des indicateurs de niveaux de service sont définis afin d'évaluer la qualité de service du Titulaire et le respect des exigences minimales pour les prestations récurrentes et dont la modalité de réception est la vérification trimestrielle de qualité de service.

En cas de défaillance constatée du Titulaire, des pénalités pour mauvaise qualité de service pourront s'appliquer conformément aux modalités décrites dans le CCAP.

Un tableau de synthèse est fourni en annexe 8 de ce livret 2 du CCTP et détaille :

- La description de chaque indicateur ;
- La méthode de calcul ;
- Le niveau de service exigé ;
- Les pénalités applicables.

11. Annexes

11.1. Annexe 1 : Présentation des standards et normes transverses, applicables à l'Amue

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 1_StandardsNormes_V1.09.pdf

11.2. Annexe 2 : Sécurité

Composé de plusieurs fichiers :

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 2.1_PlanAssuranceSecurite_V2.3.pdf
- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 2.2_ClausierSSI_V1.1.pdf
- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 2.3_Regles_Ssi_Prj_Amue_V1.7.pdf
- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 2.4_Politique_Gestion_Comptes_MotsDePasse_CCTP_v1.1.pdf

11.3. Annexe 3 : Normes de paramétrage et développement

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 3_NormesEtStandDev.zip

11.4. Annexe 4 : Processus de livraison

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 4_Processus livraison.zip

11.5. Annexe 5 : Outillage d'industrialisation des tests

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 5_Outil_industrialisation_tests.zip

11.6. Annexe 6 : Présentation de Supcoop

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 6-Pres SUPCOOP.zip



11.7. Annexe 7 : Plan d'assurance qualité Siham

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 7-PAQ.zip
- Le PAQ contient les fichiers suivants :
 - SIHAM_PAQ_PIL_PlanAssuranceQualite(V1.02)
 - Charte-support-logiciel-Siham
 - SIHAM_MOD_PIL_SuiviDesRessourcesTitulaire
 - SIHAM_MOP_MCO_ProcessusLivraisonDiffusion(V3.00)
 - SIHAM_PGD_PIL_PlanDeGestionDeLaDocumentation(V3.04)
 - SIHAM_SUP_QUA_ExempleOrdreDuJourEtTableauxDeBordCOPROJ_V1.00

11.8. Annexe 8 : Tableau des exigences de niveau de service

- Cf. fichier : 26-18-DSSE_CCTP-L2-Annexe 8-SLA