



1C avenue des Frères Lumière – CS 78242 – 69372 Lyon cedex 08

Bibliothèque Universitaire

MARCHÉ DE FOURNITURES ET DE SERVICES

MARCHÉ UJM 2026-47

**MAINTENANCE DU SYSTÈME INTÉGRÉ DE GESTION
DE BIBLIOTHÈQUE KOHA, DÉVELOPPEMENT ET PRESTATIONS ANNEXES**

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

Table des matières

ARTICLE 1 : PRÉSENTATION DE L'UNIVERSITÉ LYON 3 ET DU SERVICE COMMUN DE LA DOCUMENTATION	3
ARTICLE 2 : FONCTIONNEMENT ACTUEL KOHA.....	3
2-1 Versions et ajouts	3
2-1.1 Modules Koha utilisés.....	3
2-1.2 Modules spécifiques	4
2-1.3 Plug-ins utilisés.....	4
2-1.4 Scripts crontab.....	4
2-1.5 Patches spécifiques	5
2-1.6 Dumps	5
2-2 Environnements.....	5
2-3 Serveurs.....	5
2-3.1 Situation actuelle.....	5
2-3.2 Conditions de la future maintenance.....	6
2-4 Équipe Koha	6
ARTICLE 3 : OBJET DU MARCHÉ.....	6
3-1 LOT 1 : Maintenance évolutive et corrective du SIGB KOHA	6
3-1.1 Maintenance corrective.....	6
3-1.2 Maintenance évolutive.....	7
3-1.3 Prestations supplémentaires visant au déploiement de nouvelles fonctionnalités de kohas ou à la réinstallation du logiciel.....	7
3-2 LOT 2 : Développement du SIGB.....	7
CLAUSES DE SÉCURITÉ DES SYSTÈMES D'INFORMATIONS	8
PROTECTION DES DONNÉES PERSONNELLES	11
CONFORMITÉ AUX NORMES DE SÉCURITÉ ET HOMOLOGATION	13

ARTICLE 1 : PRÉSENTATION DE L'UNIVERSITÉ LYON 3 ET DU SERVICE COMMUN DE LA DOCUMENTATION

L'Université Jean Moulin Lyon 3 offre un espace d'apprentissage et de recherche centré sur les grandes disciplines du droit, de la gestion et des humanités. Elle propose des formations de niveau Bac +3 à Bac +8 et développe une recherche interdisciplinaire, en lien avec les grandes questions de société au sein de ses 7 écoles doctorales et 16 unités de recherche. Elle est implantée dans 3 campus. Elle accueille 27 600 étudiants et embauche 650 enseignants-chercheurs, appuyés par plus de 2 000 intervenants professionnels de 700 personnels administratifs

Le Service Commun de la Documentation (SCD) de l'Université Jean Moulin Lyon 3 assure les fonctions suivantes :

- Il gère les bibliothèques universitaires et apporte une expertise professionnelle à une vingtaine de bibliothèques de recherche avant tout pour le signalement local et national de leurs ressources,
- Il développe pour tous les usagers de l'Université des outils en réseau (catalogue général, système d'information documentaire, système de gestion pour les professionnels)

Éléments de volumétrie (données 2025 ESGBU 2026) :

Catalogue	
Notices bibliographiques	249 546
Exemplaires	321 905
Périodiques	1 217
Bibliothèques	29
Usagers	
Etudiants présents dans la base	32 743
Personnels présents dans la base	1 376 + 2 300 vacataires chargés d'enseignement
Inscrits hors université	1 554
Lecteurs actifs (au moins un emprunt en 2025)	11 492
Circulation	
Nombre de prêts et renouvellements	120 597

ARTICLE 2 : FONCTIONNEMENT ACTUEL KOHA

2-1 Versions et ajouts

Le SCD de l'Université Jean Moulin Lyon 3 utilise le SIGB Koha depuis avril 2010.

Pour son déploiement, il a été accompagné par la société Biblibre qui a ensuite assuré la maintenance du logiciel.

C'est la version communautaire 24.11 de Koha qui est installée depuis avril 2026 avec le moteur de recherche Elastic Search.

2-1.1 Modules Koha utilisés

- Acquisitions
- Autorités
- Prêt entre bibliothèques (ILL)
- Réserves de cours
- Collecte sur rendez-vous
- CAS
- Z3950,
- API
- ILS-DI
- SIP (automates de prêt).

Des règles de transferts et de réservations sont définis par site (29 sites).

Le format de catalogage est **unimarc**. La plupart du catalogage se fait dans le SUDOC avec récupération des notices bibliographiques par la suite.

Les acquisitions sont réalisées en récupérant des notices au format ISO2709 provenant des fournisseurs mais il est envisagé de passer en EDI.

2-1.2 Modules spécifiques

- SUDOC (pour les échanges de notices avec le système national de l'ABES) : <https://git.biblibre.com/biblibre/abesbnf.git>

Au cours du contrat de maintenance, le système du SUDOC va être remplacé, avec une mise en production a priori début 2028. Nous n'avons pas encore de préconisations de leur part mais il est probable que les échanges de données s'appuient sur le protocole OAI-PMH et des API. La communauté française via l'association KohaLa travaillera sur ce changement pour aider tous les établissements de l'enseignement supérieur français à adapter les échanges entre Koha et le nouveau système.

2-1.3 Plugins utilisés

- « AbesWS (fork BibLibre) » qui utilise des API de l'ABES pour enrichir les interfaces : <https://git.biblibre.com/biblibre/koha-plugin-tamil-AbesWS>
- « Patron import » pour l'import des étudiants et personnel à partir de fichiers CSV : <https://git.biblibre.com/biblibre/koha-plugin-patron-import>
- « Add-on for Lyon 3 Patron Import plugin (personnel) » qui personnalise le plugin patron-import : le code pourra être récupéré sur demande
- « Add-on for Lyon 3 Patron Import plugin (scolarité) » qui personnalise le plugin patron-import : le code pourra être récupéré sur demande
- « Transition bibliographique » qui vise à faciliter l'alignement du catalogue Koha avec les réservoirs nationaux : <https://github.com/biblibre/koha-plugin-transition-bibliographique/>
- « Users with Permissions » qui permet de visualiser tous les comptes qui ont des permissions pour l'accès à l'interface professionnelle : <https://github.com/biblibre/koha-plugin-users-with-permissions>
- « QuickItemEdit » qui permet d'ajouter un moteur de recherche aux navigateurs (Firefox ou Chrome) qui pointe vers l'édition directe d'un exemplaire : <https://github.com/oliviercrouzet/koha-plugin-quick-item-edit>
- « Koha ↔ Mir@bel » qui permet d'enrichir l'affichage avec des données du site Mir@bel (<https://reseau-mirabel.info/>) : <https://git.biblibre.com/biblibre/koha-plugin-tamil-mirabel>

2-1.4 Scripts crontab

2-1.4.1 Scripts communautaires :

- <https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/runreport.pl>
- <https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/longoverdue.pl>
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/advance_notices.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/cleanup_database.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/membership_expiry.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/overdue_notices.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/patron_email.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/process_message_queue.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/purge_suggestions.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/migration_tools/remove_unused_authorities.pl
- <https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/fines.pl>
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/search_tools/rebuild_elasticsearch.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/delete_items.pl

À venir :

- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/edi_cron.pl
- https://github.com/Koha-Community/Koha/blob/24.11.x/misc/cronjobs/marc_ordering_process.pl

Il est demandé qu'on puisse programmer n'importe quel script communautaire.

2-1.4.2 Scripts spécifiques :

- Masque automatiquement à l'OPAC les notices sans exemplaire (exceptés les périodiques) et les notices dont tous les exemplaires sont cachés par OpacHiddenItems. cf : https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=31035
- Ajout du CCODE en 319\$a en fonction de critères de la notice bibliographique
- Transfert des notices Koha créées, modifiées, supprimées à notre outil de découverte Summon (création d'un fichier ISO2709 pour les notices créées et modifiées ainsi que la création d'un fichier texte avec des biblionumber pour les notices supprimées. Les deux fichiers sont transmis par FTP)
- Ajout des notices issues d'un rapport SQL dans une liste : https://git.bibliobre.com/bibliobre/tools/src/branch/master/koha/report_to_shelf.sh
- Optimisation des tables mysql
- Mise à disposition du dump

2-1.5 Patchs spécifiques

Quelques patchs¹ spécifiques au SCD sont ajoutés et sont gérés par Bibliobre.

- Module de demande en magasin : https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=38666
- Création d'une notice bibliographique lors des demandes de PEB (ILL) pour les chapitres et les thèses : https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=38289
- Communication avec les platines RFID de bibliotheca via un webservice : <https://doc.bibliobre.com/koha/comment/faire/utiliser/la/magnetisation/demagnetisation/des/platines/avec/koha/#retour>
- Utilisation de CheckPrevCheckout en ne vérifiant que le dernier exemplaire prêté et pas tous les exemplaires rattachés à la notice bibliographique. Ce développement devrait devenir inutile en version 25.11 une fois appliqué le BZ20644 (https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=20644)

2-1.6 Dumps

Il est demandé :

- un chargement hebdomadaire de la base de production pour la charger dans la base de test ;
- d'un dump quotidien déposé dans un répertoire accessible.

2-2 Environnements

Deux environnements sont configurés : production et test et ils font partie du périmètre de la maintenance :

1. L'environnement de production est lié aux dépôts GIT de : la version de test ; Koha-community, Bibliobre.
2. L'environnement de test est lié au dépôt GIT de Koha-community et de Bibliobre.

2-3 Serveurs

2-3.1 Situation actuelle

L'instance Koha en production est sur un serveur dans le réseau interne. L'interrogation du catalogue public passe par un serveur proxy installé en DMZ (zone démilitarisée) où est installé Anubis.

L'instance de test est installée sur un serveur interne. Cette instance est toutefois utilisée non seulement pour des tests mais pour lancer des requêtes SQL assez lourdes et cela très régulièrement. Pour cette raison, il est demandé de recharger un dump de la production sur la version de tests toutes les semaines.

Tous les serveurs sont virtualisés : ils tournent sur des plateformes VMWARE

Système d'exploitation

Les OS des serveurs Ubuntu noble 64 bits.

Actuellement, les installations de Koha (production et test) sont sur un conteneur avec un accès webdav pour les échanges de fichiers (fichiers déposés ou récupérés pour traitement, xslt...)

¹ Patch : programme apportant des améliorations ou corrections au logiciel

2-3.2 Conditions de la future maintenance

Koha devra être installé sur des serveurs DEBIAN accessibles aux équipes informatiques de l'université. Il sera possible d'utiliser un conteneur docker qui devra également être accessible. Des échanges des fichiers seront à prévoir sur ce serveur (module SUDOC, envoi ou récupération de fichiers issus d'autres applications, EDI...). Le service informatique mettra à disposition les serveurs et l'installation de Koha sera faite par le prestataire de maintenance.

2-4 Équipe Koha

L'équipe est composée des 4 personnes du service d'informatique documentaire : un chef de projet et des coadministrateurs spécialisés dans certains modules. Ils devront avoir la possibilité de déclarer des incidents et poser des questions.

Les missions :

- Administration fonctionnelle de Koha.
- Rôle d'animation et de communication autour de SIGB avec les contributeurs et les utilisateurs bénéficiaires.
- Gestion des relations avec le prestataire.
- Assurer une veille sur l'évolution de Koha.
- Production de produits dérivés : listes et statistiques dans Koha.

ARTICLE 3 : OBJET DU MARCHÉ

3-1 LOT 1 : Maintenance évolutive et corrective du SIGB KOHA

Périmètre du support : la base Mysql (ou mariaDB) contenant les données, tous les modules du SIGB Koha communautaires et les spécifiques (par exemple le module SUDOC), les plugins et les couches logicielles additionnelles qui sont utilisées pour assurer le bon fonctionnement de Koha (compatibilité avec les platines et automates de prêt en RFID par exemple).

L'instance de production et l'instance de test sont couvertes par la maintenance.

Le prestataire doit proposer un support téléphonique ainsi qu'un service de déclaration d'incidents web avec une base de connaissance qui permette le suivi des actions réalisées pour leur résolution.

Documentation

Le prestataire doit fournir une documentation à jour sur tous les modules du logiciel.

3-1.1 Maintenance corrective

Le prestataire s'engage à une aide au diagnostic et à la résolution de toute difficulté de fonctionnement.

Diagnostic et contournement dans un délai de :

- Problème bloquant (=fonctionnalité inutilisable) : **J+1**.
- Problème critique (=obligation de contournement pénalisant pour l'utilisateur) : **J+2**.
- Problème mineur ou assistance (problème cosmétiques ou aide au paramétrage) : **deux semaines**.

Le prestataire assure une télémaintenance pour intervenir à distance.

Une correction définitive devra être proposée dans un délai de trois (3) mois par l'intermédiaire d'une livraison sur l'environnement de test, puis de production.

Les corrections livrées devront être proposées pour être intégrées au niveau communautaire.

Fin du contrat de maintenance : Clause de réversibilité

Le SCD devra récupérer tous les scripts, plugins ou développements spécifiques qui auront été mis en place dans le cadre de la maintenance. Ils devront être laissés sur le serveur et clairement commentés ou accessible à partir d'un dépôt git public.

3-1.2 Maintenance évolutive

Le prestataire s'engage à mettre à disposition les améliorations fonctionnelles significatives apportées au logiciel :

- Dès qu'elles sont disponibles si une anomalie a été déclarée à ce sujet, ou s'il s'agit d'une faille de sécurité,
- Lors des livraisons régulières des nouvelles versions ou mises à jour communautaires du logiciel dans les autres cas.

Des mises à jour de la version en cours devront être proposées au moins une fois par an.

Un passage vers une version supérieure doit être proposé au moins une fois par an.

3-1.3 Prestations supplémentaires visant au déploiement de nouvelles fonctionnalités de koha ou à la réinstallation du logiciel

Le SCD souhaite être accompagné dans ses projets liés à l'amélioration du SIGB Koha :

- Intégration de développement réalisé par d'autres établissements,
- Mise en place de nouveaux services,
- Réinstallation de Koha suite à la montée de version ou changement du système d'exploitation des serveurs
- Assistance à la configuration des serveurs pour optimiser le service.

Les demandes seront faites selon les besoins du SCD.

Ainsi les journées seront commandées au fur et à mesure des besoins et réglées après vérification du service fait.

Les devis devront être présentés avec de 3 types de prestations

- Conduite de projet, audit : Désignation d'un chef de projet qui suivra l'analyse de l'existant et de la faisabilité de la demande et mettra en évidence les risques potentiels. Il proposera un calendrier et un circuit de mise en place et de validation. Il sera le correspondant pendant tout le projet.
- Assistance technique : toutes prestations techniques liées à l'installation de patches, plugin spécifiques ou réinstallation de Koha
- Formation : Formation à l'administration et à la maîtrise des outils utiles pour le projet.

Le besoin est évalué à environ cinq (5) jours par an mais la totalité des jours ne sera pas obligatoirement consommée.

3-2 LOT 2 : Développement du SIGB

- Développement : toutes prestations liées au développement de nouvelles fonctionnalités qui seront proposées pour intégration à la version communautaire.

À partir d'une demande fonctionnelle décrite par le SCD, le prestataire proposera un développement qui sera proposé à la communauté sur l'outil de soumission Bugzilla et le développement sera suivi et rebasé jusqu'à intégration dans une version communautaire de Koha.

Le besoin est évalué à environ cinq (5) jours par an mais la totalité des jours ne sera pas obligatoirement consommée.

Fin du contrat : Clause de réversibilité

Le SCD devra récupérer tous les scripts, plugins ou développements spécifiques qui auront été mis en place dans le cadre de la maintenance.

CLAUSES DE SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

▪ Engagement du prestataire

Sous réserve d'engagement formel du prestataire à la « **charte d'accès distant aux ressources informatiques** » de l'université Jean Moulin Lyon 3 (annexe 1 au présent CCTP) :

Le prestataire aura un accès à distance pour livrer des correctifs ainsi que les nouvelles versions et mises à jour. Le prestataire aura une autorisation d'accès aux serveurs et un accès aux interfaces web via VPN.

Cette **Charte** réglemente :

- **Les conditions d'accès**

L'accès distant est autorisé à une personne donnée, qui est authentifiée grâce aux mécanismes inhérents aux VPN IPSec (mot de passe, certificat ou support d'authentification forte). Après s'être authentifié correctement, le prestataire a accès à des ressources définies au préalable.

Ces droits d'accès sont retirés lors de la cessation de l'activité justifiant l'accès distant et peuvent être suspendus en cas de violation de la présente charte.

- **Les droits et responsabilités du prestataire**

Le prestataire s'engage à utiliser l'accès distant aux ressources informatiques dans le cadre exclusif de son activité au sein de l'Université.

Le prestataire s'engage à ne pas effectuer, de manière volontaire, d'opérations pouvant nuire au fonctionnement du réseau de même qu'à l'intégrité des ressources informatiques.

Le prestataire s'engage à ne pas communiquer à quiconque son moyen d'authentification (mot de passe, certificat ou support d'authentification forte). Il est entièrement responsable des opérations réalisées à partir de son compte. Lorsqu'il quitte sa fonction au sein de l'université, il ne doit pas transmettre son moyen d'authentification à son successeur.

Le prestataire s'engage à installer le client VPN sur un poste sur lequel les conditions suivantes sont satisfaites :

- un anti-virus est installé, configuré correctement et dispose de mises à jour automatiques des signatures ;
- les mises à jour système sont appliquées immédiatement lorsqu'elles concernent un problème de sécurité ;
- un firewall personnel interdit les connexions entrantes (au minimum pendant les périodes où le client VPN est utilisé).

En cas de vol de son support d'authentification forte, le prestataire signalera immédiatement l'incident au RSSI (rssi@univ-lyon3.fr) et au support informatique SOS Micro : sosmicro@univ-lyon3.fr ou 04 78 78 70 77.

- **Les responsabilités de la Direction du numérique (DNUM) de l'Université Jean Moulin Lyon 3**

La Direction du numérique (DNUM) de l'Université œuvre pour assurer une qualité optimale des ressources informatiques de l'Université, tant en termes de disponibilité que de sécurité.

La Direction du numérique (DNUM) se réserve le droit de prendre les mesures nécessaires si une utilisation excessive des ressources par le prestataire nuit au bon fonctionnement général des ressources communes.

La Direction du numérique (DNUM) se doit d'avertir le prestataire de toute interruption volontaire de service, ainsi que d'en minimiser la durée.

La Direction du numérique (DNUM) peut être amenée à contrôler l'utilisation des ressources matérielles, logicielles et réseau.

- **Le respect de la loi**

La loi sanctionne certaines fraudes en matière informatique, comme l'indique la loi n°88-19 du 5 janvier 1988 (loi Godfrin), complétée par la loi n°2004-575 du 21 juin 2004 :

- Accès frauduleux à un système informatique ;
- Atteintes volontaires au fonctionnement d'un système informatique ;
- Tentative d'un de ces délits ;
- Association ou entente en vue de les commettre.

Le détail de cette loi (articles 323-1 à 323-7 du Code Pénal) est disponible à la page :

<http://www.legifrance.gouv.fr/WAspad/UnArticleDeCode?commun=CPENAL&art=323-1>

Par ailleurs, la législation interdit au prestataire de réaliser des copies de logiciels commerciaux, pour quelque usage que ce soit, ainsi que de dupliquer, distribuer ou diffuser des documents (images, sons, vidéos, ...) soumis au droit de la propriété intellectuelle.

Le détail de cette loi (articles L335-1 à 335-10 du Code de la propriété intellectuelle) est disponible à la page :

<http://www.legifrance.gouv.fr/WAspad/UnArticleDeCode?commun=CPROIN&art=L335-%25>

- **Les sanctions**

En cas de violation de la charte, l'Université pourra suspendre immédiatement les droits d'accès du prestataire aux ressources informatiques, de façon provisoire jusqu'au prononcé de la décision définitive par l'administration.

L'Université Jean Moulin est tenue par la loi de signaler toute violation des lois constatée. Elle se réserve le droit d'engager des poursuites au niveau pénal, indépendamment de toute sanction interne mise en œuvre.

- **Accès au système**

Le prestataire se porte garant de l'intégrité et de la confidentialité des données auxquelles il accède durant toute la durée du contrat. Il appartient en particulier au prestataire de vérifier que les sauvegardes nécessaires des informations de l'Université, sont disponibles de manière à permettre une reprise en cas d'incident lors de toute intervention sur le système.

- **Obligations du prestataire**

Le prestataire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art.

En particulier il s'engage à informer l'Université des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement l'Université de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

- **Points de contact sécurité**

Le prestataire s'engage à communiquer, dès qu'il en a connaissance, de tout élément touchant à la sécurité des systèmes d'information et à la protection des données à caractère personnel auprès :

- Du responsable de la sécurité des systèmes d'information de l'établissement (RSSI) : rsi@univ-lyon3.fr ;
- Du délégué à la protection des données de l'établissement (DPD) : dpd@univ-lyon3.fr .

▪ Confidentialité

Le prestataire s'engage à respecter sans aucune réserve l'annexe 2 du CCTP « clauses de confidentialité ».

Le prestataire s'engage à prévenir de tout manquement ou violation, volontaire ou non, aux termes de ce document.

▪ Audit de sécurité

L'établissement se réserve de pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

Le périmètre et la périodicité des audits de sécurité sont définis précisément par les points de contact sécurité de l'établissement comme défini dans l'article 4.3 supra.

Les audits peuvent être réalisés par l'Université, ou délégués à un tiers.

Le cas échéant, le contrôle s'effectuera par les points de contacts sécurité (RSSI et DPD) : visite des locaux du prestataire avec interviews individuelles des membres des équipes du prestataire, accès aux machines mises à la disposition du prestataire.

Cette visite sera notifiée au prestataire selon un délai de 15 jours.

La pratique de tests intrusifs par le prestataire est interdite sur tout ou partie du système d'informations de l'établissement.

L'Université doit se réserver le droit de requérir l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

▪ Sécurité des développements applicatifs

Le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre avec en particulier :

- Environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
- Contrôle rigoureux des entrées utilisateurs ;
- Sécurisation des accès aux fonctions d'administration ;
- Installation du minimum de fonctions nécessaires lors de l'installation ;
- Principe du moindre privilège ;
- Utilisation de mots de passe dans le code interdit ;
- Mise en œuvre d'une gestion efficace des erreurs.

Pour la mise en œuvre de technologies web, les développements doivent s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

La recette de l'application comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du prestataire.

▪ Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.

En cas d'évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

PROTECTION DES DONNÉES PERSONNELLES

▪ Identification des parties

Responsable de traitement : l'Université Jean Moulin Lyon 3 (ci-après UJML3), à travers son Service Commun de la Documentation (SCD), sise 1C avenue des frères Lumière, CS 78242, 69372 Lyon Cedex 08, représenté par son Président ;

Le prestataire sous-traitant au sens RGPD : [à renseigner]

Nom ou Raison sociale :

Adresse(s) :

Téléphone :

Adresse électronique :

N° SIRET :

CODE APE :

N° TVA intracommunautaire :

▪ Objet

Dans le cadre de leurs relations contractuelles, les parties prennent les mesures techniques et organisationnelles appropriées de manière à répondre aux exigences des textes en vigueur relatifs au traitement de données à caractère personnel, en particulier au Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données (RGPD) et à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (LIL).

Les présentes clauses ont pour objet de préciser les obligations des parties et conditions dans lesquelles sont réalisées les traitements de données à caractère personnel définis ci-après.

▪ Description du traitement faisant l'objet de la sous-traitance pour le compte de l'UJML3

Le sous-traitant est autorisé à traiter pour le compte de l'UJML3, les données à caractère personnel nécessaires à la fourniture du service de maintenance et aux prestations visant au déploiement de nouvelles versions et nouvelles fonctionnalités. À ce titre, le sous-traitant est autorisé à avoir accès et à consulter les ressources informatiques de l'UJML3.

▪ Obligations du sous-traitant vis-à-vis de l'UJML3

Le sous-traitant traite les données pour les seules finalités qui font l'objet de la sous-traitance décrite dans le présent CCTP. Il traite les données conformément aux instructions documentées de l'UJML3. Il prend toutes les mesures requises en matière de sécurité des données en vertu de l'article 32 du RGPD et de la charte d'accès distant aux ressources informatiques de l'UJML3.

Le sous-traitant veille, en particulier, à ce que les personnes autorisées à traiter les données à caractère personnel en vertu des présentes clauses :

- S'engagent contractuellement à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
- Reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

Le sous-traitant prend en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut définies à l'article 25 du RGPD.

- Sous-traitance le cas échéant

Le sous-traitant est autorisé à faire appel à l'entité [...] (ci-après « le sous-traitant ultérieur ») pour mener les activités de traitement suivantes :

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique de l'UJML3.

Le sous-traitant ultérieur est tenu de respecter les obligations des présentes clauses pour le compte et selon les instructions de l'UJML3. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant l'UJML3 de l'exécution par le sous-traitant ultérieur de ses obligations.

- Chef de conformité

Dans le cadre du présent marché, les parties conviennent de point de contact concernant les problématiques relatives à la protection des données personnelles :

Pour l'Université Jean Moulin Lyon3 : le délégué à la protection des données personnelles désigné, dpd@univ-lyon3.fr

Pour le prestataire : [...] :

CONFORMITÉ AUX NORMES DE SÉCURITÉ ET HOMOLOGATION

Le logiciel proposé doit être conforme aux normes internationales de sécurité de l'information, en particulier la norme ISO/IEC 27001 et au règlement général sur la protection des données RGPD.

Le fournisseur doit démontrer que le logiciel et ses processus de développement respectent les critères suivants :

- **Gestion de la Sécurité de l'Information** : le fournisseur doit disposer d'une documentation complète de la politique de sécurité, des processus et des contrôles en place pour protéger les données.
- **Évaluation et Gestion des Risques** : le logiciel doit avoir été soumis à une évaluation des risques de sécurité, avec des mesures de protection adaptées pour atténuer ces risques. Le fournisseur doit fournir des preuves de cette évaluation, incluant les méthodologies employées et les résultats obtenus.
- **Contrôles de Sécurité Intégrés** : le logiciel doit inclure des contrôles de sécurité, tels que le contrôle d'accès, la gestion des incidents de sécurité, la cryptographie, la gestion des vulnérabilités, et la protection des données en transit et au repos.
- **Homologation de Sécurité** : le fournisseur doit être en mesure de fournir tous les documents nécessaires pour l'obtention d'un accord d'homologation de sécurité, conformément au décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics. Cela inclut, mais n'est pas limité à, des rapports de tests de sécurité, des audits de conformité, et des déclarations de sécurité.
- **Maintien et Mise à Jour de la Sécurité** : le fournisseur doit s'engager à maintenir et mettre à jour régulièrement le logiciel pour assurer sa conformité continue aux normes de sécurité, y compris la gestion proactive des vulnérabilités et la fourniture de correctifs de sécurité en temps opportun.