LYON 1 - UNIVERSITE CLAUDE BERNARD

ACQUISITION ET MAINTENANCE DU CONTROLE D'ACCES



CAHIER DES CHARGES TECHNIQUES PARTICULIERES

SOMMAIRE

SOMMAIRE **2**
PREAMBULE **5**
ELEC.1. PRESENTATION DE L'UNIVERSITE CLAUDE BERNARD LYON 1 5
ELEC.2. CONTEXTE GENERAL DU CONTROLE D'ACCES 5
ELEC.3. ÉTAT ACTUEL DU SYSTEME 6
ELEC.4. ENSEIGNEMENTS DES AUDITS ET ETUDES PREALABLES 7
ELEC.5. OBJECTIFS TECHNIQUES ET TRAJECTOIRE RECHERCHEE 8
A. Assurer la continuité d'exploitation 9
B. Maintenir une expertise forte de l'environnement SIPASS 9
C. Réduire progressivement la dette technique 10
D. Préserver les infrastructures de terrain existantes 10
E. Préparer la montée en sûreté des périmètres sensibles 11
F. Construire une architecture pérenne et évolutive 11
INTRODUCTION **13**
ELEC.6. PRESENTATION GENERALE DU MARCHE 13
A. Objet du marché 13
B. Principes d'organisation des prestations 13
C. Allotissement du marché et modalités 14
D. Profil et compétences attendues des titulaires 15
E. Principes de gouvernance 16
ELEC.7. PHILOSOPHIE ET AMBITION DU MARCHE 18
ELEC.8. PHILOSOPHIE OPERATIONNELLE DU MARCHE 18
ELEC.9. RÉFÉRENCES RÉGLEMENTAIRES ET NORMATIVES 19
A. Généralités 19
B. Textes réglementaires 20
C. Normes relatives aux installations électriques 20
D. Normes relatives aux réseaux de communication et systèmes de contrôle d'accès 21
E. Normes et référentiels spécifiques aux systèmes de sûreté 21
F. Compatibilité réglementaire des ouvrages 21
G. Evolution des textes 21
ELEC.10. ATTENDUS RELATIFS AUX OFFRES ET AU MÉMOIRE TECHNIQUE 22
A. Principes généraux 22
B. Objectifs du mémoire technique 22
C. Trame imposée du mémoire technique 22
D. Cohérence des réponses 25
EXPLOITATION ET MAINTIEN EN CONDITION OPERATIONNELLE DES INSTALLATIONS DE CONTRÔLE D'ACCES **26**
ELEC.11. PRINCIPES GENERAUX D'EXPLOITATION ET DE MAINTIEN EN CONDITION OPÉRATIONNELLE 26
A. Objet du domaine 26
B. Principes généraux d'exploitation 26
C. Périmètre des prestations 27
D. Maintenance corrective 32

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

E. Gestion patrimoniale et documentaire 36
F. Gestion de l'obsolescence 36
ELEC.12. PRESCRIPTIONS GÉNÉRALES D'INTERVENTION ET D'EXPLOITATION SUR LES SITES DE L'UNIVERSITÉ 36
A. Objet du chapitre 36
B. Horaires d'intervention et continuité d'activité 37
C. Prise en compte des usagers et activités de l'Université 37
D. Gestion des accès, circulation et stationnement 37
E. Interventions sur les parkings et accès véhicules 38
F. Accès aux zones sensibles 38
G. Coordination des interventions et coactivité 39
H. Protection des infrastructures existantes 39
I. Continuité des dispositifs de sûreté 39
J. Gestion documentaire des interventions 39
K. Contrôles, essais et réception des installations 40
L. Prescriptions relatives aux infrastructures de câblage 40
M. Respect des référentiels de l'Université 42
N. Réversibilité opérationnelle 42
ELEC.13. GESTION DES DEMANDES, DES EVOLUTIONS ET DES TRAVAUX ANNEXES 42
A. Principes généraux 42
B. Gestion des demandes d'intervention 42
C. Principes techniques applicables aux diverses évolutions 43
D. Études préalables 43
E. Gestion des devis 43
F. Présentation et contenu des devis 44
G. Gestion des demandes d'évolution 46
H. Commission de Contrôle d'Accès 46
I. Modélisation des niveaux de sûreté 46
J. Déploiement de solutions spécifiques 47
K. Gestion multi-solutions 48
L. Validation des évolutions 48
ELEC.14. PRESCRIPTIONS TECHNIQUES APPLICABLES AUX TRAVAUX D'ÉVOLUTION, DE CRÉATION ET DE RENOUVELLEMENT DES INSTALLATIONS DE CONTRÔLE D'ACCÈS 48
A. Objet du chapitre 48
B. Principes généraux de conception 48
C. Prescriptions relatives aux équipements de contrôle d'accès 49
D. Contrôle d'accès sur les portes 50
E. Équipements minimaux d'une porte contrôlée 50
F. Alimentation électrique et continuité de service 50
G. Réseaux de communication et infrastructures de terrain 51
H. Réalisation des câblages 52
I. Réception technique des travaux 53
J. Dossier des ouvrages exécutés 53
EXPERTISE FONCTIONNELLE, LOGICIELLE ET GESTION DES DONNEES 54

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

ELEC.15. PRINCIPES GENERAUX DE MAITRISE FONCTIONNELLE DE L'ENVIRONNEMENT SIPASS 54
A. Objet du domaine 54
B. Principe de compétence et d'organisation 54
C. Mise à niveau de l'environnement SIPASS et sécurisation de l'infrastructure 54
D. Administration fonctionnelle de la plateforme SIPASS 56
E. Gestion des habilitations et des droits d'accès 56
F. Administration des groupes d'accès 57
G. Gestion des référentiels et synchronisations 57
H. Gestion des populations particulières 57
I. Qualité, cohérence et audit des données 57
J. Support expert SIPASS 58
EVOLUTIONS ET MIGRATION DE LA SOLUTION EXISTANTE 59
ELEC.16. PRINCIPES DIRECTEURS D'UNE MIGRATION TECHNOLOGIQUE 59
A. Objet du domaine 59
B. Principes directeurs de la trajectoire d'évolution 59
C. Rationalisation et maîtrise du nombre d'unités de traitement 59
D. Principe d'ouverture et d'interopérabilité 60
E. Convergence et supervision des environnements 61
F. Périmètres à sûreté renforcée 61
G. Compatibilité avec les trajectoires ANSSI et NIS2 62
H. Maîtrise des coûts récurrents d'exploitation 62

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

PREAMBULE

ELEC.1. PRESENTATION DE L'UNIVERSITE CLAUDE BERNARD LYON 1

L'Université Claude Bernard Lyon 1 est un établissement public à caractère scientifique, culturel et professionnel exerçant ses missions de formation, de recherche et d'innovation dans les domaines des sciences, des technologies, de la santé et du sport.

Son patrimoine immobilier est réparti sur 3 campus principaux et 11 sites géographiques situés en région Rhône-Alpes. Il représente une surface foncière totale de 824 616 m², une surface bâtie de 465 001 m² et plus de 26 000 locaux. Ce patrimoine accueille des activités d'enseignement, de recherche, de services administratifs et de vie étudiante. Il se caractérise par une grande diversité d'usages et de niveaux de sensibilité, intégrant notamment des locaux d'enseignement, des plateformes techniques, des laboratoires de recherche, des animaleries, des installations techniques et plusieurs périmètres soumis à des exigences de sécurité renforcées.

La diversité et l'étendue de ce patrimoine conduisent l'Université à exploiter des dispositifs de sûreté adaptés à des contextes fonctionnels, techniques et réglementaires variés, allant des bâtiments d'enseignement courants jusqu'aux infrastructures de recherche présentant des enjeux particuliers de protection des personnes, des biens et des activités scientifiques.

L'Université mène depuis plusieurs années une politique de sécurisation progressive de ses bâtiments, de protection des personnes, des biens et des activités de recherche, tout en veillant à préserver les conditions d'ouverture et d'accessibilité propres à un établissement d'enseignement supérieur.

ELEC.2. CONTEXTE GENERAL DU CONTROLE D'ACCES

Afin de mieux répondre à ses besoins de sûreté, de gestion des flux et de protection de ses activités d'enseignement et de recherche, l'Université Claude Bernard Lyon 1 s'est progressivement dotée d'un système de contrôle d'accès centralisé permettant la gestion des accès aux bâtiments, aux locaux sensibles et aux infrastructures associées.

Déployé initialement à partir de 2008 autour de la solution SIPASS, ce système s'est développé au fil des années, de manière empirique et éparse, pour accompagner les évolutions du patrimoine immobilier, l'augmentation du nombre d'usagers ainsi que les besoins spécifiques des composantes, laboratoires et services de l'établissement.

Le contrôle d'accès constitue aujourd'hui un outil essentiel au fonctionnement quotidien de l'Université. Il participe à la sécurisation des personnes et des biens, à la protection des activités de recherche, à la gestion des accès aux locaux sensibles ainsi qu'à la maîtrise des flux sur l'ensemble du patrimoine immobilier.
Le système doit répondre aujourd'hui à une grande diversité de situations et prendre en charge des populations hétérogènes composées notamment :

- de personnels de l'Université ;
- d'étudiants ;
- de chercheurs et enseignants associés ;
- de personnels hébergés ou mutualisés avec d'autres établissements ;
- de personnels de recherche appartenant à des organismes partenaires ;
- de prestataires ;
- de visiteurs disposant d'autorisations temporaires.

Au-delà de la diversité des populations gérées, le système doit également prendre en compte des modalités d'accès et d'administration différenciées selon les usages, les bâtiments et les niveaux de sensibilité concernés. Certaines populations bénéficient ainsi de mécanismes largement automatisés reposant sur les référentiels institutionnels de l'Université, tandis que d'autres nécessitent des traitements spécifiques, des habilitations particulières ou des modalités d'administration décentralisées.

Le système assure notamment :

- la gestion automatisée des droits des personnels et étudiants à partir du référentiel de l'établissement ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la gestion spécifique de populations extérieures ou hébergées nécessitant des processus spécifiques ;
- la gestion des accès temporaires liés aux visiteurs et intervenants occasionnels ;
- la gestion des accès prestataires, notamment pour les parkings et infrastructures techniques au travers de dispositifs combinant badge, code PIN ou mécanismes d'autorisation spécifiques ;
- la prise en compte de besoins particuliers associés à certains laboratoires, plateformes techniques, animaleries ou périmètres de recherche présentant des contraintes d'exploitation ou de sûreté renforcées ;
- la coexistence de règles d'accès différenciées selon les sites, les bâtiments et les catégories d'usagers.

Cette diversité implique une gestion fine des droits d'accès, des habilitations et des mécanismes de synchronisation, reposant sur des processus fortement intégrés au système d'information de l'établissement.

L'environnement actuel s'appuie sur les référentiels SIHAM, APOGEE et UNICAMPUS permettant la constitution d'un référentiel unique alimentant le système de contrôle d'accès. Un connecteur spécifique assure aujourd'hui le lien entre ce référentiel et la solution SIPASS exploitée par l'Université.

ELEC.3. ÉTAT ACTUEL DU SYSTEME

La solution actuelle est basée sur le logiciel Sipass dans sa version 2.76.

Le dispositif actuellement exploité couvre :

- 11 sites géographiques ;
- 110 bâtiments équipés ;
- 1 637 lecteurs de contrôle d'accès ;
- 44 barrières de contrôle d'accès véhicules ;
- plusieurs dizaines d'unités de traitement locales (UTL) ;
- plusieurs milliers d'équipements périphériques associés aux accès.

Le système gère actuellement plus de 53 000 porteurs de badges, avec des variations importantes liées au calendrier universitaire. Lors des périodes de rentrée ou de traitements massifs des données de scolarité et des ressources humaines, le volume de personnes gérées peut atteindre ou dépasser 65 000 individus.

Les habilitations reposent sur plus de 3 000 groupes d'accès, constitués de populations variées pouvant être issues :

- des référentiels de l'Université ;
- d'organismes de recherche partenaires ;
- d'établissements hébergés ;
- de communautés scientifiques extérieures ;
- ou de populations temporaires nécessitant des droits spécifiques.

Le système doit ainsi supporter des mécanismes complexes de gestion des accès, combinant des populations permanentes, temporaires et mixtes, avec des niveaux de sensibilité différents selon les bâtiments et les activités hébergées.

L'architecture actuelle repose principalement sur :

- une solution logicielle centralisée de contrôle d'accès ;
- des UTL réparties sur les différents sites (89) ;
- des infrastructures de terrain largement construites autour de communications série de type RS485 avec une structure assez homogène, fondée sur des séries d'automates de 2 lecteurs (quelques fois 8);
- des lecteurs fonctionnant en technologie 13,56 MHz.

Le parc de badges est lui-même hétérogène et comprend plusieurs technologies compatibles 13,56 MHz, déployées au fil des différentes évolutions du système depuis sa mise en place.

Les solutions cibles proposées dans le cadre du présent marché pour la future migration devront prendre en compte cette diversité et garantir la continuité de fonctionnement des populations existantes pendant toute la durée du contrat.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Enfin, le système assure le contrôle d'accès de plusieurs périmètres à sensibilité renforcée, notamment certains locaux de recherche, plateformes techniques et zones soumises à des contraintes réglementaires particulières (ZRR).

Ces périmètres présentent des exigences spécifiques en matière de sûreté, de traçabilité et d'évolution du niveau de sécurité, qui devront être intégrées dans les orientations techniques et organisationnelles proposées par les titulaires du marché.

ELEC.4. ENSEIGNEMENTS DES AUDITS ET ETUDES PREALABLES

Les audits techniques, organisationnels et fonctionnels réalisés par l'Université ont permis d'établir un état des lieux détaillé du système de contrôle d'accès actuellement déployé et d'identifier les enjeux structurants qui conditionneront son évolution dans les années à venir.

Ces travaux ont confirmé que le dispositif actuellement en place constitue un système mature, robuste et fortement intégré aux processus métiers de l'établissement. Déployé depuis plus de quinze ans, il assure quotidiennement la gestion des accès de plusieurs dizaines de milliers d'usagers répartis sur l'ensemble du patrimoine universitaire.

Son architecture repose sur une forte mutualisation des infrastructures, des mécanismes d'autonomie locale éprouvés ainsi qu'une intégration poussée avec les systèmes d'information de l'Université.
Les audits ont toutefois mis en évidence que cette architecture a progressivement atteint certaines limites fonctionnelles, organisationnelles et technologiques qu'il est nécessaire de corriger.

Cette situation résulte notamment :

- de l'absence d'une roadmap d'évolution clairement définie sur le long terme de la part du constructeur;
- du vieillissement progressif de certains composants matériels et logiciels ;
- de l'abandon ou de la fin de support de certaines gammes de matériels ;
- de l'évolution des exigences de cybersécurité ;
- de dépendances technologiques importantes ;
- de la difficulté croissante à maintenir certaines technologies historiques ;
- de l'émergence de nouveaux besoins de sûreté insuffisamment pris en compte par les architectures initialement déployées.

Les audits ont ainsi démontré que les difficultés rencontrées aujourd'hui ne résultent pas principalement des infrastructures de terrain elles-mêmes mais de l'absence de trajectoire d'évolution formalisée permettant d'accompagner durablement les transformations du patrimoine, des usages et des exigences de sécurité de l'établissement.

Les études ont également démontré que le contrôle d'accès ne peut être considéré comme une simple infrastructure composée de lecteurs, de contrôleurs et de dispositifs de verrouillage.

Son fonctionnement repose sur un ensemble cohérent associant :

- une plateforme logicielle centralisée de gestion des accès ;
- des mécanismes de synchronisation avec les systèmes d'information de l'établissement ;
- des référentiels de personnes et de groupes ;
- des processus automatisés d'attribution et de retrait des droits ;
- des infrastructures de terrain assurant l'exécution des décisions de contrôle d'accès.

À ce titre, la continuité de fonctionnement du système dépend autant de la maîtrise des équipements déployés sur le terrain que de la maîtrise des composants logiciels, des données et des processus fonctionnels constituant le cœur du dispositif.

Les analyses réalisées ont notamment confirmé le rôle central de la solution SIPASS dans l'architecture actuelle. Celle-ci assure aujourd'hui la gestion des porteurs, des habilitations, des groupes d'accès, des interfaces avec le système d'information ainsi qu'une part importante des mécanismes d'administration du contrôle d'accès.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Dans ce contexte, les audits ont mis en évidence la nécessité de préserver, pendant les prochaines années, une expertise avancée de cet environnement afin de garantir :

- le maintien en condition opérationnelle du système actuel ;
- la continuité des processus métiers existants ;
- l'intégrité des données d'habilitation ;
- la stabilité des interfaces avec les applications métiers ;
- la préparation et la sécurisation des futures opérations de transformation.

Les études ont également démontré que très peu d'acteurs du marché disposent aujourd'hui d'une compétence approfondie et durable sur cet environnement historique. Cette situation constitue un facteur de vigilance majeur pour l'Université et devra être prise en compte dans l'organisation du futur marché.

Enfin, les audits ont confirmé que les infrastructures de terrain actuellement déployées conservent de nombreux atouts en matière de résilience, de maintien en condition opérationnelle. Les analyses concluent qu'une stratégie de remplacement systématique et immédiat du patrimoine existant ne constituerait ni la solution la plus efficiente, ni la plus pertinente au regard des objectifs poursuivis par l'établissement.

Les audits conduisent ainsi l'Université à privilégier une démarche de transformation progressive fondée sur :

- la préservation des infrastructures présentant un niveau de performance satisfaisant ;
- la réduction progressive de la dette technique ;
- la rationalisation des architectures ;
- la maîtrise des dépendances technologiques ;
- le renforcement des capacités de supervision et de pilotage ;
- la mise en place d'une trajectoire d'évolution cohérente et durable ;
- la préparation de futurs niveaux de sûreté adaptés aux différents enjeux du patrimoine universitaire.

L'objectif poursuivi par le présent marché n'est pas uniquement de corriger les conséquences du vieillissement du système actuel mais de construire un cadre d'évolution permettant à l'Université de retrouver durablement la maîtrise de sa feuille de route technique, fonctionnelle et sécuritaire pour les années à venir.

ELEC.5. OBJECTIFS TECHNIQUES ET TRAJECTOIRE RECHERCHEE

Le présent marché s'inscrit dans la stratégie de maîtrise et d'évolution du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.

Au regard de la place centrale qu'occupe aujourd'hui le contrôle d'accès dans le fonctionnement quotidien de l'établissement, l'Université souhaite disposer d'un cadre contractuel lui permettant simultanément d'assurer la continuité d'exploitation du système existant, de maîtriser les risques liés à son vieillissement progressif et de préparer les évolutions nécessaires pour répondre aux enjeux futurs de sûreté, de cybersécurité et d'exploitation.

Les analyses réalisées ont montré que le dispositif actuel demeure pleinement opérationnel et continue de répondre à une grande partie des besoins de l'établissement. Elles ont toutefois mis en évidence l'apparition progressive de facteurs de risque liés à l'obsolescence de certains composants, à la dépendance vis-à-vis de technologies historiques et à l'évolution des exigences de sécurité applicables aux établissements d'enseignement supérieur et de recherche.

Dans ce contexte, l'Université n'a pas retenu une stratégie de rupture reposant sur le remplacement intégral et immédiat du système existant. Elle privilégie au contraire une démarche de transformation progressive, pilotée et maîtrisée, permettant d'inscrire les évolutions du contrôle d'accès dans une trajectoire durable et soutenable sur un plan technique et économique.

Cette trajectoire repose sur un principe directeur : **assurer le maintien en condition opérationnelle du système actuel, préserver la continuité des services rendus aux utilisateurs et réduire progressivement la dette technique, tout en préparant l'émergence d'une architecture plus ouverte, plus pérenne et capable de répondre aux futurs enjeux de sûreté de l'établissement.**

Le présent marché constitue ainsi à la fois :

- un dispositif de maintien et de sécurisation du système actuellement exploité ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- un outil de maîtrise et de réduction progressive des risques techniques identifiés par les audits ;
- un cadre d'accompagnement des évolutions fonctionnelles nécessaires à l'Université ;
- un levier de transformation permettant de préparer et de conduire, dans la durée, les futures opérations de modernisation du contrôle d'accès.

Dans cette perspective, les prestations attendues devront permettre de concilier continuité d'exploitation, maîtrise des investissements, préservation du patrimoine existant et capacité d'évolution du système sur le long terme, tout en garantissant un niveau de service compatible avec les contraintes d'un établissement accueillant quotidiennement plusieurs dizaines de milliers d'usagers et supportant des activités de recherche à différents niveaux de sensibilité.

6 points doivent être retenus dans le cadre de ce projet.

A. Assurer la continuité d'exploitation

Le système de contrôle d'accès actuellement déployé constitue une infrastructure stratégique de l'Université Claude Bernard Lyon 1. Il participe quotidiennement à la sécurisation des personnes, des biens, des activités d'enseignement et des activités de recherche, tout en assurant la gestion des accès pour plusieurs dizaines de milliers d'usagers répartis sur l'ensemble du patrimoine immobilier de l'établissement.

Compte tenu de son niveau de diffusion et de son intégration aux processus métiers de l'Université, toute interruption, dégradation ou perte de maîtrise de ce système est susceptible d'avoir un impact direct sur l'exploitation des bâtiments, l'accès aux locaux concernés, le fonctionnement des services administratifs ainsi que la continuité des activités pédagogiques et scientifiques.

Dans ce contexte, le maintien de la disponibilité, de la stabilité et des performances du système constitue une exigence fondamentale du présent marché.

Les futurs titulaires devront être en mesure d'assurer la continuité opérationnelle de l'ensemble de la chaîne de contrôle d'accès, comprenant notamment :

- les infrastructures de terrain ;
- les unités de traitement et équipements associés ;
- les plateformes logicielles de supervision et d'administration ;
- les bases de données et référentiels d'habilitations ;
- les mécanismes d'échanges et de synchronisation avec le système d'information ;
- les outils d'exploitation, de gestion et de pilotage du contrôle d'accès ;
- les procédures permettant l'administration et le maintien des droits des usagers.

Cette obligation de continuité s'applique à l'ensemble des phases du marché, y compris lors des opérations de maintenance, d'évolution, de renouvellement ou de migration.

Les solutions et organisations proposées devront démontrer leur capacité à garantir la continuité du service, à limiter les interruptions d'exploitation et à assurer la coexistence maîtrisée des composants historiques et des composants nouvellement déployés pendant toute la durée de la trajectoire de transformation retenue par l'Université.

L'objectif recherché est de permettre à l'établissement de conduire les évolutions nécessaires de son système de contrôle d'accès sans dégrader la qualité de service actuellement rendue aux usagers et sans compromettre les exigences de sûreté associées à ses activités.

B. Maintenir une expertise forte de l'environnement SIPASS

Compte tenu de la place centrale de SIPASS dans l'architecture actuelle et de la durée prévisible de coexistence entre les systèmes historique et cible, l'Université considère que la maîtrise de cette solution constitue un enjeu stratégique du marché, nécessitant sa mise en exergue dans le cadre d'un lot spécifique.
Les prestations attendues ne se limitent donc pas à la maintenance matérielle des installations existantes. Elles couvrent également :

- l'administration fonctionnelle de la plateforme ;
- le support logiciel avancé ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- le maintien des interfaces avec le système d'information ;
- l'accompagnement des évolutions fonctionnelles nécessaires au maintien du service ;
- l'assistance aux opérations de reprise et de migration des données.

Cette expertise devra être maintenue pendant toute la durée nécessaire à la migration complète du système.

C. Réduire progressivement la dette technique

Les analyses réalisées ont mis en évidence la nécessité d'engager une trajectoire de renouvellement progressive du système de contrôle d'accès afin de traiter les situations d'obsolescence identifiées et de restaurer durablement les capacités d'évolution et de maintien en condition opérationnelle du dispositif.

Cette démarche vise prioritairement les composants matériels et logiciels dont le niveau d'ancienneté, la disponibilité des pièces de rechange, les conditions de support ou les contraintes de cybersécurité sont susceptibles de constituer un facteur de risque pour l'exploitation future du système.

L'Université souhaite toutefois que cette transformation soit conduite selon une logique de transition maîtrisée, garantissant la continuité de fonctionnement des services rendus aux utilisateurs et la préservation des processus métiers actuellement supportés par la plateforme de contrôle d'accès.

Les opérations de renouvellement, de modernisation ou de migration devront ainsi être conçues de manière à :

- maintenir un niveau élevé de disponibilité des infrastructures tout au long de la transition ;
- éviter toute rupture de service susceptible d'impacter les activités d'enseignement, de recherche ou de gestion de l'établissement ;
- assurer la continuité des mécanismes de gestion des habilitations et des droits d'accès ;
- préserver l'intégrité des données et des configurations existantes ;
- sécuriser les phases de coexistence entre les composants historiques et les composants nouvellement déployés ;
- limiter les impacts organisationnels et techniques sur les équipes d'exploitation.

L'objectif poursuivi est de réduire progressivement la dette technique du système tout en améliorant son niveau global de maintenabilité, de résilience, de sécurité et de pérennité.

Le futur marché devra ainsi offrir à l'Université la capacité d'engager des évolutions successives, compatibles avec ses contraintes opérationnelles et budgétaires, sans remettre en cause la continuité du service ni les investissements déjà réalisés.

D. Préserver les infrastructures de terrain existantes

Les audits et études préalables ont mis en évidence la valeur technique, fonctionnelle et économique des infrastructures actuellement déployées. Ils ont notamment démontré que certaines composantes du système, en particulier les infrastructures de câblage et les architectures de communication de terrain, conservent un haut niveau de pertinence au regard des besoins de l'établissement et ne constituent pas, à ce jour, un facteur limitant pour les évolutions envisagées.

Dans ce contexte, l'Université privilégie une démarche de transformation fondée sur la valorisation des investissements réalisés et la préservation des infrastructures existantes lorsqu'elles répondent aux exigences de performance, de fiabilité et de pérennité attendues.

Les solutions proposées devront ainsi rechercher prioritairement :

- la réutilisation des infrastructures de câblage existantes lorsque leur état et leurs caractéristiques techniques le permettent ;
- la conservation des architectures de communication de terrain ayant démontré leur robustesse et leur résilience opérationnelle ;
- la limitation des opérations de recâblage, de reprise d'infrastructures ou de reconstruction complète des réseaux de terrain ;
- la réduction des impacts sur les bâtiments exploités, les activités d'enseignement, les plateformes de recherche et les services administratifs ;
- la maîtrise du coût global de transformation du système sur l'ensemble de son cycle de vie.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

L'Université privilégie ainsi une logique d'évolution maîtrisée plutôt qu'une stratégie de remplacement systématique des infrastructures en place.
Toute proposition reposant sur une refonte massive des architectures de terrain devra démontrer de manière argumentée les bénéfices techniques, opérationnels, sécuritaires et économiques apportés par cette approche au regard de la conservation de l'existant.

Cette orientation vise à garantir une transition soutenable, à limiter les risques liés aux opérations de migration et à préserver les qualités de robustesse, de maintenabilité et d'exploitation qui caractérisent aujourd'hui le système de contrôle d'accès de l'établissement.

E. Préparer la montée en sûreté des périmètres sensibles

Le patrimoine de l'Université accueille des activités présentant des niveaux de sensibilité hétérogènes, allant des espaces d'enseignement et de vie universitaire aux plateformes techniques, laboratoires de recherche, infrastructures critiques et périmètres soumis à des exigences réglementaires particulières.

Dans ce contexte, le futur système de contrôle d'accès devra permettre une gestion différenciée des niveaux de sûreté, adaptée à la criticité réelle des bâtiments, des locaux et des activités hébergées.
Les solutions proposées devront offrir la capacité de mettre en œuvre, au sein d'une architecture cohérente et unifiée, plusieurs niveaux de protection répondant aux besoins spécifiques de chaque périmètre, tout en conservant des modes d'administration, de supervision et d'exploitation homogènes à l'échelle de l'établissement.

L'Université souhaite notamment disposer d'une trajectoire lui permettant de renforcer progressivement le niveau de sécurité de certains espaces sensibles, en particulier les zones de recherche stratégiques, les plateformes techniques critiques, les infrastructures à enjeux et les périmètres susceptibles d'être soumis à des exigences renforcées de sûreté ou de cybersécurité.

Cette montée en exigence devra pouvoir être réalisée de manière progressive, ciblée et maîtrisée, sans remettre en cause les investissements réalisés sur le reste du patrimoine et sans imposer une transformation simultanée de l'ensemble du système.

Les architectures proposées dans le cadre de la migration future devront ainsi démontrer leur capacité à intégrer, selon les besoins de l'établissement, des mécanismes compatibles avec les recommandations de l'ANSSI, tout en garantissant la continuité d'exploitation des infrastructures existantes et la cohérence globale du dispositif de contrôle d'accès.

F. Construire une architecture pérenne et évolutive

Enfin, l'Université souhaite se doter d'une architecture de contrôle d'accès pérenne, ouverte et évolutive, capable d'accompagner durablement les transformations de son patrimoine immobilier, de ses activités de recherche et de son système d'information.

Les solutions cibles mises en œuvre devront démontrer leur capacité à s'inscrire dans une trajectoire d'évolution de long terme reposant sur les principes suivants :

- une interopérabilité native permettant l'intégration et la coexistence de composants issus de plusieurs constructeurs ou éditeurs ;
- des interfaces ouvertes, documentées et maintenues, facilitant l'interconnexion avec les systèmes d'information de l'établissement ainsi qu'avec des équipements tiers de sûreté, de sécurité ou de supervision ;
- une maîtrise des infrastructures réseau, privilégiant les architectures concentrées, limitant le nombre d'équipements communicants et réduisant les flux permanents nécessaires au fonctionnement du système ;
- une indépendance technologique renforcée, permettant à l'Université de faire évoluer ses équipements, ses composants logiciels ou ses infrastructures sans dépendance exclusive à un constructeur, un intégrateur ou une gamme matérielle unique ;
- la capacité à exploiter, au sein d'une architecture centralisée et cohérente, plusieurs générations ou familles d'équipements répondant à des besoins fonctionnels ou sécuritaires différents ;
- une évolutivité progressive vers des architectures de sûreté renforcée, compatibles avec les recommandations de l'ANSSI et permettant, lorsque les enjeux le justifient, la mise en œuvre

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

de dispositifs spécifiques sur les périmètres sensibles sans remise en cause de l'architecture globale du système.

Le futur marché devra ainsi constituer à la fois un dispositif de maintien en condition opérationnelle du système existant, un cadre de maîtrise de la dette technique identifiée par les audits et un levier de transformation permettant la mise en œuvre progressive de la trajectoire technique et sécuritaire définie par l'Université.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

INTRODUCTION

ELEC.6. PRESENTATION GENERALE DU MARCHE

A. Objet du marché

Le présent marché a pour objet d'assurer le maintien en condition opérationnelle, l'exploitation, l'évolution et la transformation progressive du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.
Les prestations attendues couvrent l'ensemble du cycle de vie du système de contrôle d'accès, depuis les activités quotidiennes de maintenance et d'exploitation jusqu'aux opérations de modernisation et de renouvellement des infrastructures.

Le marché vise à garantir la continuité des services actuellement rendus aux usagers tout en accompagnant la trajectoire technique définie par l'établissement dans le cadre des audits et études préalables réalisés dernièrement.

Dans cette perspective, l'Université attend des titulaires une capacité à intervenir simultanément sur les dimensions :

- techniques ;
- logicielles ;
- fonctionnelles ;
- organisationnelles ;
- patrimoniales ;
- sécuritaires ;

✓ du système de contrôle d'accès.

B. Principes d'organisation des prestations

Les prestations attendues s'articulent autour de trois domaines d'intervention complémentaires permettant d'assurer simultanément l'exploitation du système existant, la préservation des compétences critiques et la préparation de ses évolutions futures.

- Domaine n°1 : Exploitation et maintien en condition opérationnelle

Ce domaine couvre l'ensemble des prestations nécessaires au maintien du niveau de service attendu par l'Université.

Il comprend notamment :

- la maintenance préventive ;
- la maintenance corrective ;
- les interventions d'urgence ;
- la maintenance des équipements de terrain ;
- la maintenance des dispositifs de contrôle d'accès véhicules ;
- la maintenance des équipements associés ;
- la tenue à jour de la documentation technique ;
- la gestion patrimoniale des équipements.

L'objectif est d'assurer la disponibilité permanente du système et de préserver ses capacités opérationnelles pendant toute la durée du marché.

- Domaine n°2 : Expertise fonctionnelle, logicielle et gestion des données

Ce domaine couvre l'ensemble des prestations relatives au fonctionnement du cœur applicatif du système de contrôle d'accès.

Il comprend notamment :

- l'administration de la solution existante ;
- le maintien des mécanismes de gestion des habilitations ;
- l'exploitation des interfaces avec le système d'information ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- le maintien des processus automatisés ;
- l'administration des données de contrôle d'accès ;
- le support fonctionnel avancé ;
- l'expertise technique de la solution actuellement déployée.

Ce domaine constitue un élément critique de la stratégie retenue par l'Université dans la mesure où il conditionne la continuité des services pendant toute la durée de la trajectoire de migration.

- Domaine n°3 : Évolutions, renouvellement et transformation du système

Ce domaine couvre les prestations d'ingénierie et de transformation nécessaires à l'évolution du contrôle d'accès.
Il comprend notamment :

- les études d'architecture ;
- les opérations de renouvellement des infrastructures ;
- les projets de modernisation ;
- les migrations progressives ;
- les opérations de reprise de données ;
- le déploiement de nouvelles technologies ;
- l'accompagnement des évolutions liées aux enjeux de sûreté et de cybersécurité.

Ce domaine a pour vocation d'accompagner la réduction progressive de la dette technique du système tout en préparant son évolution vers une architecture plus pérenne et adaptée aux futurs besoins de l'établissement.

C. Allotissement du marché et modalités

Compte tenu des compétences spécifiques nécessaires à l'exploitation, à l'administration et à l'évolution du système de contrôle d'accès de l'Université Claude Bernard Lyon 1, le marché est structuré en plusieurs lots correspondant aux principaux domaines d'intervention identifiés dans le cadre des audits réalisés.
Cette organisation vise à garantir la mobilisation des compétences adaptées à chaque domaine tout en assurant la continuité d'exploitation du système et la cohérence des évolutions futures.

* C1 - Allotissement

Le découpage retenu est le suivant :

Lot	Intitulé	Finalité	Ambition
Lot n°1	Exploitation et maintien en condition opérationnelle	Assurer la disponibilité, la maintenance, l'exploitation et la pérennité des infrastructures physiques du système de contrôle d'accès	Maintenir
Lot n°2	Expertise fonctionnelle, logicielle et maîtrise de l'environnement SIPASS	Assurer l'administration de la plateforme actuelle, la gestion des habilitations, des données et des interfaces avec le système d'information	Maîtriser
Lot n°3	Évolutions, renouvellement et transformation du système	Accompagner les études, les évolutions architecturales, les opérations de migration et les projets de modernisation	Transformer

Le présent marché repose sur trois ambitions complémentaires :

- Maintenir les capacités opérationnelles du système existant et garantir la continuité de service ;
- Maîtriser les mécanismes fonctionnels, les données, les habilitations et l'environnement SIPASS qui constituent aujourd'hui le cœur du dispositif ;
- Transformer progressivement le système afin de réduire la dette technique, accompagner la montée en sûreté des périmètres sensibles et préparer l'émergence d'une architecture ouverte, interopérable et durable.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

*C2 - Répartition des domaines de compétences

Domaine de compétence	Lot 1	Lot 2	Lot 3
Maintenance préventive	X		
Maintenance corrective	X		
Astreinte technique	X		
Gestion patrimoniale	X		
Contrôle d'accès piétons	X		
Contrôle d'accès véhicules	X		
Gestion des infrastructures RS485	X		
Administration SIPASS		X	
Gestion des habilitations		X	
Gestion des groupes d'accès		X	
Gestion des données		X	
Interfaces SIHAM / APOGEE / UNICAMPUS		X	
Expertise fonctionnelle avancée		X	
Études d'évolution			X
Études d'architecture			X
Renouvellement des infrastructures			X
Migration et coexistence des solutions			X
Montée en sûreté des périmètres sensibles			X
Compatibilité ANSSI			X

D. Profil et compétences attendues des titulaires

*D1 - Possibilités de réponses

Les candidats pourront répondre à un ou plusieurs lots.

Compte tenu des audits relatifs à la spécificité de l'environnement actuellement exploité, l'Université attire l'attention des candidats sur la nécessité de disposer de l'ensemble des compétences requises pour le ou les lots auxquels ils répondent.

Lorsque certaines compétences ne sont pas maîtrisées directement par le candidat, celui-ci pourra s'appuyer sur un groupement ou sur des expertises complémentaires lui permettant de garantir la couverture complète des prestations attendues.

En particulier, la maîtrise de l'environnement SIPASS constitue une compétence spécifique dont la disponibilité devra être démontrée par les candidats répondant aux prestations relevant du lot n°2.

*D2 - Profil et compétences attendues des titulaires

Compte tenu de la criticité du système de contrôle d'accès pour le fonctionnement de l'Université, les candidats devront démontrer leur capacité à intervenir dans un environnement multi-sites, fortement exploité et présentant des enjeux significatifs de sûreté, de continuité d'activité et de protection des activités de recherche.
Les titulaires devront disposer de compétences leur permettant d'assurer :

- l'exploitation et le maintien en condition opérationnelle d'infrastructures de contrôle d'accès de grande dimension ;
- l'administration et le support de plateformes logicielles de contrôle d'accès ;
- la gestion de patrimoines techniques complexes et hétérogènes ;
- la conduite d'opérations d'évolution, de modernisation et de migration ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- l'accompagnement de la maîtrise d'ouvrage dans ses choix techniques et organisationnels.

Les candidats devront justifier de références significatives dans des environnements présentant des contraintes comparables à celles de l'Université, notamment :

- établissements d'enseignement supérieur ;
- organismes de recherche ;
- établissements de santé ;
- établissements multi-sites ;
- patrimoines comportant des infrastructures critiques ou des zones à accès restreint.

L'Université reconnaît que certaines compétences spécifiques, notamment celles relatives à l'environnement SIPASS et à ses mécanismes d'intégration, peuvent être portées par des acteurs spécialisés distincts des intégrateurs intervenant sur les infrastructures de terrain.
À ce titre, les candidats pourront s'appuyer sur :

- des cotraitants ;
- des sous-traitants spécialisés ;
- des partenaires techniques ;
- des groupements d'expertises complémentaires.

Ils devront toutefois démontrer la cohérence de l'organisation proposée ainsi que leur capacité à mobiliser durablement l'ensemble des compétences nécessaires pendant toute la durée du marché.

L'Université sera particulièrement attentive à la capacité des candidats à combiner :

- expertise terrain des systèmes de contrôle d'accès ;
- maîtrise des infrastructures techniques associées ;
- compétences fonctionnelles et applicatives ;
- capacité de conseil et d'assistance à la décision ;
- aptitude à accompagner les trajectoires d'évolution retenues par l'établissement;
- outil de gestion de la maintenance et du parc global.

E. Principes de gouvernance

Compte tenu de la criticité du système de contrôle d'accès pour le fonctionnement de l'établissement et de son caractère transverse, le pilotage du présent marché repose sur une gouvernance partagée entre plusieurs directions de l'Université, chacune intervenant dans son domaine de compétence.

Chacune de ces composantes est représentée au sein d'un Commission de Contrôle d'Accès (CCA) chargée de statuer sur les demandes de travaux et d'extension (voir section E. chapitre ELEC.13)

Les titulaires devront intégrer cette organisation dans leur mode de fonctionnement et être en mesure de travailler en coordination permanente avec la gouvernance collégiale dans l'exploitation, l'évolution et la sécurisation du système.

Direction du Patrimoine

La Direction du Patrimoine est chargée du pilotage patrimonial, budgétaire et opérationnel des infrastructures de contrôle d'accès.
À ce titre, elle assure notamment :

- le pilotage financier du marché et le suivi de son exécution budgétaire ;
- la planification, le suivi des opérations de maintenance, de renouvellement et de travaux ;
- la relation avec les utilisateurs, les occupants des bâtiments et les services demandeurs ;
- le suivi des interventions réalisées sur le terrain ;
- la gestion et le pilotage du patrimoine matériel associé au contrôle d'accès ;
- la validation des opérations de maintenance préventive et corrective ;
- le suivi des opérations de renouvellement, de modernisation et de remplacement des équipements ;
- la coordination des interventions avec les autres opérations de maintenance ou de travaux menées sur le patrimoine immobilier ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la maîtrise d'ouvrage des interventions réalisées dans le périmètre des installations électriques, des réseaux courants faibles et des infrastructures techniques associées au contrôle d'accès ;
- le contrôle de la conformité des travaux réalisés ainsi que la validation des DOE, inventaires et documents patrimoniaux produits dans le cadre du marché.

La Direction du Patrimoine constitue l'interlocuteur privilégié des titulaires pour toutes les prestations relatives aux équipements physiques, aux interventions sur site et à la gestion patrimoniale du système.
Plusieurs responsables sont affectés aux campus en tant qu'interlocuteur privilégié.

○ Direction des Systèmes d'Information

La Direction des Systèmes d'Information est garante de l'exploitation technique et fonctionnelle des composants numériques du système de contrôle d'accès.

Elle assure notamment :

- l'administration et l'exploitation des composants logiciels ;
- le maintien des interfaces avec le système d'information de l'Université ;
- la gestion des référentiels d'identités et des mécanismes de synchronisation ;
- la cohérence des données et des habilitations ;
- la supervision des plateformes logicielles ;
- l'intégration des évolutions techniques dans l'écosystème numérique de l'établissement ;
- l'application des exigences de cybersécurité relevant du système d'information.

Elle constitue l'interlocuteur de référence pour tous les sujets relatifs à l'architecture logicielle, aux données, aux interfaces, aux mécanismes de gestion des accès et aux évolutions numériques du dispositif.

○ Direction Sécurité

La Direction Sécurité est garante de la cohérence des dispositifs de contrôle d'accès avec les objectifs de sûreté et de sécurité de l'établissement.

À ce titre, elle participe notamment :

- à la définition des orientations stratégiques en matière de contrôle d'accès ;
- à la qualification des besoins de sûreté / sécurité ;
- à la définition des niveaux de sécurité attendus ;
- à l'identification des périmètres sensibles ou critiques ;
- à la définition des politiques d'accès pour les zones à risques et les situations exceptionnelles ;
- à l'élaboration des exigences applicables aux zones à enjeux particuliers ;
- aux arbitrages relatifs aux évolutions du système ayant un impact sur la sûreté des personnes, des biens ou des activités de recherche.

La Direction Sécurité contribue également à la définition de la trajectoire de montée en sûreté de certains périmètres et à l'identification des besoins d'évolution associés.

○ Principe de pilotage partagé

Les titulaires reconnaissent que le système de contrôle d'accès constitue un système transverse associant des enjeux :

- patrimoniaux ;
- techniques ;
- organisationnels ;
- réglementaires ;
- de sûreté ;
- de cybersécurité.

À ce titre, les décisions structurantes relatives aux évolutions du système, aux stratégies de maintenance, aux opérations de transformation ou aux évolutions des niveaux de sécurité pourront être prises conjointement par la Direction du Patrimoine, la Direction des Systèmes d'Information et la Direction Sécurité.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Les titulaires devront être en capacité de présenter leurs analyses, recommandations et propositions à chacune de ces directions et d'adapter leurs interventions aux orientations validées dans le cadre de cette gouvernance partagée.

ELEC.7. PHILOSOPHIE ET AMBITION DU MARCHE

Au-delà de la seule gestion des accès physiques, l'Université souhaite inscrire le présent marché dans une démarche globale de pilotage de la sûreté de ses infrastructures, de ses activités et de son patrimoine scientifique.

Le contrôle d'accès constitue aujourd'hui un système d'information à part entière, au carrefour des enjeux patrimoniaux, numériques, sécuritaires et organisationnels de l'établissement.

À ce titre, l'Université ne recherche pas uniquement un dispositif permettant de contrôler l'ouverture ou la fermeture des accès, mais une solution capable de produire de la connaissance, d'améliorer la compréhension des usages, de renforcer la maîtrise des risques et d'accompagner les décisions relatives à la sécurisation de son patrimoine.

Le futur système devra ainsi permettre de dépasser une logique traditionnelle de gestion des accès pour évoluer vers une approche davantage orientée :

- pilotage de la sûreté ;
- connaissance des périmètres et des populations ;
- maîtrise des risques ;
- aide à la décision ;
- traçabilité des événements ;
- supervision des infrastructures critiques ;
- valorisation des données produites par le système.

L'Université attend notamment que les informations issues du contrôle d'accès puissent contribuer à une meilleure compréhension du fonctionnement de ses bâtiments, de ses espaces sensibles et de ses activités de recherche, dans le respect du cadre réglementaire applicable et des exigences de protection des données.

Cette orientation implique une **capacité des titulaires à accompagner l'établissement dans une démarche d'amélioration continue**, fondée sur l'exploitation intelligente des données, le partage des informations, la communication entre les acteurs et l'anticipation des évolutions futures.

Le contrôle d'accès est ainsi considéré comme l'un des composants structurants de la politique de sûreté de l'Université et comme un outil contribuant à la protection des personnes, des biens, des activités scientifiques et des infrastructures critiques.

Le présent marché vise donc à construire les conditions d'une transition progressive entre une logique historique de pure gestion technique des accès vers une logique intégrée de pilotage de la sûreté à l'échelle de l'établissement.

ELEC.8. PHILOSOPHIE OPERATIONNELLE DU MARCHE

L'Université Claude Bernard Lyon 1 considère désormais le contrôle d'accès comme un composant structurant de sa politique globale de sûreté et de protection de ses activités.

Historiquement conçu comme un outil de gestion des accès physiques aux bâtiments et aux locaux, le système de contrôle d'accès est aujourd'hui devenu un élément central de l'organisation de l'établissement. Il participe quotidiennement à la protection des personnes, des biens, des activités de recherche, des infrastructures techniques et des espaces à enjeux particuliers.

Dans un contexte marqué par l'évolution des risques, la diversification des usages, l'augmentation des exigences de cybersécurité et le développement de périmètres de recherche sensibles, l'Université souhaite faire évoluer progressivement son approche vers une logique de **pilotage global de la sûreté**.

Le présent marché ne se limite donc pas à la fourniture, à l'installation ou à la maintenance d'équipements de contrôle d'accès, ni à la seule gestion des autorisations d'ouverture des portes et des accès véhicules.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Il vise à doter l'établissement d'un dispositif lui permettant :

- de garantir la continuité de fonctionnement d'un système devenu critique pour les activités d'enseignement, de recherche et d'administration ;
- de maintenir un haut niveau de disponibilité des infrastructures existantes tout au long de leur trajectoire d'évolution ;
- d'améliorer la maîtrise de son patrimoine technique, de son cycle de vie et de sa dette technologique ;
- de disposer d'une connaissance fiable et documentée de ses équipements, de leurs états, de leurs performances et de leurs besoins de renouvellement ;
- de renforcer la qualité, la cohérence et l'exploitation des données relatives aux accès, aux habilitations et aux populations autorisées ;
- d'améliorer la visibilité sur les usages réels des bâtiments, des espaces et des infrastructures sensibles ;
- de disposer d'indicateurs permettant d'éclairer les décisions relatives aux politiques d'accès et aux investissements futurs ;
- d'adapter les niveaux de sûreté aux enjeux réels des bâtiments, des activités et des populations concernées ;
- d'accompagner la montée en exigences de certains périmètres sensibles, notamment les espaces de recherche, les plateformes techniques critiques et les zones soumises à des contraintes réglementaires ou de sécurité particulières ;
- de construire une architecture évolutive, capable d'intégrer progressivement de nouveaux besoins, de nouvelles technologies et de nouveaux niveaux d'exigence.

L'Université attend également que le système de contrôle d'accès contribue à une meilleure communication entre les différents acteurs impliqués dans la gestion de la sûreté.

Les solutions de services proposées devront ainsi favoriser :

- le partage d'informations entre les directions concernées ;
- la traçabilité des décisions et des interventions ;
- la consolidation des données utiles au pilotage ;
- la capacité à produire des analyses et des tableaux de bord ;
- l'amélioration continue du niveau de connaissance du patrimoine et des risques associés.

Dans cette perspective, les titulaires ne devront pas se limiter à une logique d'exécution de prestations techniques. Ils devront être en mesure d'apporter une véritable expertise d'accompagnement fondée sur :

- le conseil ;
- l'analyse ;
- l'anticipation des risques ;
- la proposition d'améliorations ;
- le partage d'expérience ;
- l'assistance à la décision ;
- la capacité à inscrire leurs actions dans une vision cohérente à l'échelle du patrimoine universitaire.

Le contrôle d'accès est ainsi considéré par l'Université comme un système participant directement à la protection des personnes, des biens, des données, des activités de recherche et des infrastructures critiques de l'établissement.

Le présent marché devra permettre de faire évoluer progressivement le dispositif actuel vers une approche intégrée où les équipements, les données, les processus, les usages et les objectifs de sûreté concourent à une même finalité : disposer d'un système de contrôle d'accès performant, maîtrisé, évolutif et véritablement au service du pilotage de la sûreté de l'Université.

ELEC.9. RÉFÉRENCES RÉGLEMENTAIRES ET NORMATIVES

A. Généralités

Le titulaire du présent marché est réputé connaître l'ensemble des textes réglementaires, normes, règles de l'art et prescriptions techniques applicables aux prestations qui lui sont confiées, notamment en terme de RGPD et confidentialité.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Il devra assurer, sans que cette liste soit limitative, toutes les prestations nécessaires à la réalisation complète des ouvrages, à leur protection, à leur maintien en parfait état pendant les travaux ainsi qu'à leur parfaite conformité jusqu'à la réception des prestations.

Le titulaire devra notamment intégrer dans son offre l'ensemble des dispositions techniques, administratives et financières nécessaires au respect des textes réglementaires et normatifs applicables.

Les installations réalisées devront être conformes aux normes et textes réglementaires dans leur dernière édition en vigueur à la date de remise des offres.

Le titulaire sera également tenu au respect de tous les textes publiés postérieurement à la remise des offres lorsque leur application est rendue obligatoire avant la réalisation des prestations.

Les ouvrages devront être exécutés conformément aux règles de l'art applicables aux installations électriques, aux systèmes de contrôle d'accès, aux réseaux de communication et aux équipements de sûreté électronique.

B. Textes réglementaires

*B1. Décrets relatifs aux installations électriques

Sans que cette liste soit exhaustive, les installations devront respecter les dispositions résultant notamment des textes suivants :

- Décret n°88-1056 du 14 novembre 1988 relatif à la protection des travailleurs dans les établissements mettant en œuvre des courants électriques ;
- Décret n°2010-1016 du 30 août 2010 relatif aux obligations de l'employeur pour l'utilisation des installations électriques des lieux de travail ;
- Décret n°2010-1017 du 30 août 2010 relatif aux obligations des maîtres d'ouvrage lors de la construction ou de l'aménagement de bâtiments destinés à recevoir des travailleurs ;
- Décret n°2010-1018 du 30 août 2010 relatif à la prévention des risques électriques dans les lieux de travail.

*B2. Code du travail

Le titulaire devra respecter l'ensemble des dispositions applicables du Code du Travail relatives notamment :

- à la sécurité des travailleurs ;
- aux interventions sur installations électriques ;
- aux habilitations électriques ;
- à la prévention des risques ;
- aux travaux réalisés en site occupé.

C. Normes relatives aux installations électriques

*C1. Courants forts – Basse tension

Les ouvrages devront notamment respecter :

- NF C 15-100 et ses amendements ;
- NF C 15-103 ;
- l'ensemble des prescriptions applicables aux installations électriques basse tension dans les établissements recevant du public et les bâtiments universitaires.

Toute alimentation nécessaire au fonctionnement des installations de contrôle d'accès devra être conçue conformément à ces référentiels.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

D. Normes relatives aux réseaux de communication et systèmes de contrôle d'accès

*D1. Courants faibles

Les ouvrages devront notamment être compatibles avec les prescriptions résultant des documents suivants :

- NF EN 60950-1 et ses additifs ;
- UTE C 98-011 ;
- ISO/IEC 11801-1 ;
- ISO/IEC 11801-3 ;
- IEC 60603-7-51 ;
- IEC 60512-99-001 ;
- EN 50288 parties 2-1 et 2-2 ;
- NF C 15-900.

Les infrastructures de communication mises en œuvre devront être adaptées aux échanges de données, à l'alimentation des équipements connectés, à la supervision ainsi qu'aux contraintes de cybersécurité applicables aux systèmes de sûreté de l'Université.

E. Normes et référentiels spécifiques aux systèmes de sûreté

Les installations de contrôle d'accès devront être réalisées conformément :

- aux règles de l'art applicables aux systèmes électroniques de sûreté ;
- aux référentiels APSAD applicables aux installations de contrôle d'accès lorsqu'ils existent ;
- aux préconisations des fabricants des équipements installés ;
- aux exigences de cybersécurité définies par l'Université ;
- aux prescriptions de la Direction des Systèmes d'Information ;
- aux prescriptions de la Direction Sécurité.

F. Compatibilité réglementaire des ouvrages

Le titulaire devra vérifier que les équipements proposés sont compatibles avec :

- les contraintes ERP ;
- les règles de sécurité incendie ;
- les dispositifs d'évacuation ;
- les prescriptions d'accessibilité ;
- les réglementations relatives aux personnes à mobilité réduite ;
- les contraintes des laboratoires et espaces de recherche ;
- les prescriptions applicables aux zones sensibles et aux zones à régime restrictif.

Aucun équipement ne pourra être installé lorsqu'il est susceptible de remettre en cause les exigences réglementaires de sécurité ou d'exploitation du bâtiment concerné.

*G. Evolution des textes

La liste ci-dessus n'est pas limitative.

Le titulaire devra appliquer :

- toutes les normes rendues obligatoires ;
- tous les arrêtés, décrets et circulaires applicables aux prestations ;
- tous les documents techniques unifiés et guides professionnels de référence ;
- toutes les évolutions réglementaires publiées avant la réalisation des travaux concernés.

Il demeure seul responsable de la conformité réglementaire des ouvrages réalisés jusqu'à leur réception.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

ELEC.10. ATTENDUS RELATIFS AUX OFFRES ET AU MÉMOIRE TECHNIQUE

A. *Principes généraux*

Le présent marché porte sur un système de contrôle d'accès constituant un élément stratégique du fonctionnement de l'Université Claude Bernard Lyon 1.

Les candidats devront démontrer leur compréhension des enjeux présentés dans le présent CCTP ainsi que leur capacité à accompagner l'établissement dans ses trois ambitions structurantes :

- maintenir le niveau de service et la continuité d'exploitation ;
- maîtriser les composantes fonctionnelles, applicatives et organisationnelles du système ;
- accompagner la transformation progressive du patrimoine de contrôle d'accès.

Les offres devront être rédigées de manière claire, argumentée et directement exploitable par les services de l'Université.

Les réponses génériques, catalogues commerciaux, documentations constructeurs non contextualisées ou simples reprises du CCTP sans analyse associée seront considérées comme insuffisantes.

B. *Objectifs du mémoire technique*

Le mémoire technique a pour objectif de permettre à l'Université d'apprécier :

- la compréhension du contexte ;
- la qualité de l'organisation proposée ;
- la maîtrise des technologies concernées ;
- la capacité à maintenir l'existant ;
- la capacité à accompagner les évolutions futures ;
- la qualité du conseil apporté à la maîtrise d'ouvrage ;
- la cohérence de la vision proposée par le candidat.

Les candidats devront démontrer leur capacité à intervenir dans un environnement :

- multi-sites ;
- multi-acteurs ;
- fortement exploité ;
- intégrant des activités de recherche ;
- intégrant des périmètres à sensibilité renforcée.

C. *Trame imposée du mémoire technique*

Afin de permettre une analyse homogène des offres, les candidats devront impérativement structurer leur mémoire technique selon le plan suivant.

* *Partie 1 - Compréhension du contexte et des enjeux*

Le candidat présentera :

- sa compréhension du patrimoine de l'Université ;
- sa compréhension des enjeux de sûreté ;
- sa compréhension de l'organisation actuelle ;
- sa compréhension des contraintes liées à SIPASS ;
- sa compréhension des enjeux de dette technique ;
- sa compréhension des enjeux de migration et de transformation.

Aussi, le candidat présentera :

- trois exemples d'alertes patrimoniales émises chez des clients comparables ;
- un exemple de démarche de réduction de dette technique ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- un exemple de stratégie de migration progressive ;
- un exemple d'aide à la décision apportée à une maîtrise d'ouvrage.

Une attention particulière sera portée à la capacité du candidat à démontrer sa compréhension du contexte spécifique de l'Université.

* *Partie 2 - Organisation générale et gouvernance*

Le candidat présentera :

- son organisation générale dédiée ;
- les moyens humains affectés spécifiquement au marché ;
- les fonctions des intervenants ;
- les modalités de pilotage ;
- les modalités de coordination avec l'Université ;
- les modalités de remplacement des intervenants ;
- les modalités de continuité d'activité.

Un organigramme nominatif ou fonctionnel sera fourni.

* *Partie 3 - Maintien en condition opérationnelle (lot 1)*

Le candidat détaillera :

- son organisation de maintenance ;
- son organisation de maintenance préventive ;
- son organisation de maintenance corrective ;
- sa méthodologie de gestion des urgences ;
- sa méthode de suivi patrimonial ;
- sa méthode de gestion documentaire ;
- les outils de pilotage proposés ;
- les indicateurs de performance suivis.

* *Partie 4 - Gestion des données et expertise fonctionnelle (lot 2)*

Cette partie est particulièrement attendue pour les candidats répondant au domaine relatif à l'environnement SIPASS.

Le candidat présentera :

- les compétences mobilisées ;
- son expérience de SIPASS ;
- sa méthodologie d'administration ;
- sa méthodologie de gestion des habilitations ;
- sa maîtrise des référentiels ;
- sa maîtrise des synchronisations ;
- sa démarche de qualité des données ;
- sa capacité à accompagner les futures opérations de migration.

* *Partie 5 - Gestion des évolutions et des travaux (lot 3)*

Le candidat détaillera :

- sa méthodologie d'analyse des besoins ;
- sa méthodologie d'étude ;
- sa méthodologie de chiffrage ;
- sa gestion des travaux ;
- sa gestion des interfaces avec les autres corps d'état ;
- sa gestion de la documentation de fin d'opération ;
- sa méthodologie de réception.

Mais aussi :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- sa méthodologie de conception des accès ;
- sa doctrine de choix des verrouillages ;
- sa méthodologie de réalisation des extensions ;
- sa gestion des alimentations ;
- sa méthode de recette ;
- sa production documentaire.

* *Partie 6 - Vision stratégique et trajectoire de transformation (lot 1, 2, 3)*

Le candidat exposera sa vision concernant :

- la réduction progressive de la dette technique ;
- la préservation du patrimoine existant ;
- la réutilisation des infrastructures de terrain ;
- la rationalisation des architectures ;
- l'ouverture des systèmes ;
- l'interopérabilité ;
- la supervision consolidée ;
- la coexistence de plusieurs solutions ;
- les futures opérations de migration.

Mais aussi :

- sa politique de standardisation des matériels ;
- sa méthodologie de réduction du nombre de références ;
- sa méthodologie de gestion des pièces de rechange ;
- sa stratégie de lutte contre l'obsolescence ;
- sa vision de la maintenabilité à long terme ;
- les indicateurs patrimoniaux qu'il juge pertinents

Le candidat expliquera comment son offre répond concrètement aux enseignements des audits mentionnés dans le présent CCTP.

Cette partie devra permettre à l'Université d'apprécier la capacité du candidat à accompagner la trajectoire de transformation décrite dans le présent marché.

* *Partie 7 - Sûreté, cybersécurité et environnements sensibles*

Le candidat détaillera :

- sa prise en compte des zones sensibles ;
- sa prise en compte des ZRR ;
- sa prise en compte des infrastructures critiques ;
- son approche de la cybersécurité ;
- sa connaissance des recommandations ANSSI ;
- sa capacité à accompagner les trajectoires associées à NIS2 ;
- sa gestion des accès sensibles et des opérations critiques.

* *Partie 8 - Outils, reporting et pilotage*

Le candidat détaillera :

- les outils proposés ;
- les modalités de reporting ;
- les indicateurs produits ;
- les tableaux de bord proposés ;
- les modalités de partage d'information ;
- les outils de gestion des demandes ;
- les outils de gestion patrimoniale.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

* *Cas pratiques*

L'Université se réserve la possibilité de demander aux candidats la production de cas pratiques ou mises en situation permettant d'évaluer leur compréhension des enjeux du marché.

Ces cas pratiques pourront notamment porter sur :

- une opération de maintenance complexe ;
- une évolution de bâtiment ;
- la gestion d'un périmètre de recherche sensible ;
- la coexistence de plusieurs solutions de contrôle d'accès ;
- une trajectoire de migration progressive ;
- la supervision consolidée de plusieurs environnements.

D. Cohérence des réponses

Les candidats veilleront à assurer une cohérence entre :

- leur mémoire technique ;
- leur organisation ;
- leurs moyens humains ;
- leurs références ;
- leur offre financière ;
- les matériels ou solutions proposés.

L'Université pourra considérer comme insuffisante toute offre présentant des incohérences significatives entre les engagements annoncés et les moyens réellement mobilisés.

L'analyse financière pourra être réalisée indépendamment sur :

- les prestations forfaitaires ;
- la maintenance corrective ;
- la main d'œuvre ;
- les fournitures ;
- les études ;
- les prestations de migration.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

LOT1 : EXPLOITATION ET MAINTIEN EN CONDITION OPERATIONNELLE DES INSTALLATIONS DE CONTRÔLE D'ACCES

ELEC.11. PRINCIPES GENERAUX D'EXPLOITATION ET DE MAINTIEN EN CONDITION OPÉRATIONNELLE

A. Objet du domaine

Le présent domaine couvre l'ensemble des prestations nécessaires au maintien en condition opérationnelle du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.

Il constitue le socle de continuité du présent marché et vise à garantir la disponibilité, la fiabilité, la sécurité et les performances des installations de contrôle d'accès exploitées par l'Université, indépendamment des opérations d'évolution, de renouvellement, de modernisation ou de transformation qui pourront être engagées pendant la durée du contrat.

Les prestations attendues portent sur l'ensemble des infrastructures contribuant au fonctionnement quotidien du contrôle d'accès, qu'elles soient matérielles, d'exploitation ou organisationnelles.
Le périmètre de maintenance est réputé couvrir l'ensemble du patrimoine de contrôle d'accès exploité par l'Université pendant toute la durée du marché.

À ce titre, les éventuelles évolutions technologiques, opérations de migration, déploiements de solutions spécifiques ou remplacements d'équipements intervenant au cours du marché ne pourront être considérés comme réduisant de plein droit le périmètre des prestations de maintien en condition opérationnelle.

Sauf disposition contraire validée par l'Université, tout équipement nouvellement déployé, remplacé ou migré et intégré au patrimoine de contrôle d'accès devra être pris en compte dans le dispositif de maintenance et d'exploitation défini au présent chapitre.

L'Université se réserve notamment la possibilité de faire coexister plusieurs architectures ou solutions de contrôle d'accès sur différents périmètres de son patrimoine. Cette coexistence ne saurait remettre en cause les obligations de maintenance, de continuité d'exploitation et de gestion patrimoniale applicables aux équipements confiés au titulaire.

L'objectif poursuivi est de garantir un niveau de service homogène à l'échelle de l'établissement, compatible avec les exigences d'exploitation d'une université multi-sites accueillant plusieurs dizaines de milliers d'usagers et supportant des activités de recherche présentant différents niveaux de sensibilité.

B. Principes généraux d'exploitation

Le titulaire devra assurer le maintien permanent de la capacité opérationnelle du système de contrôle d'accès. À ce titre, il devra mettre en œuvre l'ensemble des moyens humains, matériels, organisationnels et méthodologiques permettant :

- d'assurer la continuité du service ;
- de prévenir les situations de dégradation ;
- d'anticiper les risques d'indisponibilité ;
- de maintenir les performances du système ;
- de préserver les capacités de fonctionnement des équipements existants ;
- de contribuer à la maîtrise de la dette technique identifiée par l'Université.

La maintenance ne devra pas être limitée à une approche corrective mais devra s'inscrire dans une démarche proactive de surveillance, d'analyse, d'amélioration continue et de conseil à travers une logique de maintenance préventive dynamique.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

C. Périmètre des prestations

Le présent domaine couvre l'ensemble des équipements et infrastructures physiques participant au fonctionnement du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.

Il comprend les équipements de terrain, les infrastructures de communication associées, les dispositifs de verrouillage, les accès véhicules ainsi que l'ensemble des éléments nécessaires au fonctionnement opérationnel du système de contrôle d'accès.
Le titulaire devra assurer la maintenance, l'exploitation, le maintien en condition opérationnelle, le suivi patrimonial et l'évolution des équipements décrits ci-après.

*C.1 Infrastructures de contrôle d'accès des personnes

Cette catégorie regroupe l'ensemble des équipements permettant l'identification, l'autorisation et le contrôle des accès piétons.
Elle intègre l'ensemble des dispositifs suivants :

- lecteurs de badges ;
- lecteurs avec clavier intégré ;
- les futurs dispositifs de lecture spécifiques déployés dans les périmètres sensibles.
- unités de traitement locales (UTL) ;
- contrôleurs d'accès ;
- modules de portes ;
- modules d'entrées/sorties ;
- modules d'extension ;
- interfaces de communication associées.

Elle intègre de même l'ensemble des organes de commande et de détection suivants :

- boutons poussoirs de sortie ;
- boutons de demande d'ouverture ;
- déclencheurs manuels associés ;
- contacts de porte ;
- capteurs d'état ;
- dispositifs de détection liés aux automatismes d'accès.
- Organes de condamnation et de verrouillage
- gâches électriques ;
- ventouses électromagnétiques ;
- serrures motorisées ;
- dispositifs de condamnation électrique ;
- équipements électromécaniques associés.

*C.2 Contrôle des accès véhicules

Cette catégorie regroupe l'ensemble des équipements assurant le contrôle, la sécurisation et la gestion des flux véhicules sur les différents sites de l'Université.

Elle comprend notamment :

- Les barrières levantes ;
- bornes de contrôle d'accès ;
- armoires de commande ;
- variateurs ;
- cellules de sécurité ;
- boucles de détection ;
- détecteurs de présence ;
- dispositifs de protection mécanique.
- Organes d'autorisation
- lecteurs de badges ;
- claviers codés ;
- dispositifs de commande spécifiques.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

* C.3 Réseaux et infrastructures de terrain

Cette catégorie couvre les infrastructures permettant l'échange d'informations entre les équipements du système de contrôle d'accès.

- ✓ Réseaux de communication

  - bus RS485 ;
  - liaisons de communication terrain ;
  - convertisseurs ;
  - interfaces série ;
  - passerelles de communication associées.

L'Université attache une importance particulière au maintien de la fiabilité et de la disponibilité de ces infrastructures, qui constituent un élément structurant de l'architecture actuellement déployée.

- ✓ Infrastructures techniques

  - coffrets de contrôle d'accès ;
  - armoires techniques ;
  - baies dédiées au contrôle d'accès ;
  - équipements de raccordement associés.

* C.4 Alimentation et continuité énergétique

Cette catégorie regroupe l'ensemble des équipements participant à l'alimentation électrique, à l'autonomie énergétique et à la continuité de fonctionnement du système de contrôle d'accès.

Elle comprend notamment :

- alimentations stabilisées ;
- alimentations secourues ;
- chargeurs ;
- batteries ;
- dispositifs de protection électrique ;
- équipements de secours nécessaires au maintien du fonctionnement des accès.

Le titulaire devra porter une attention particulière au maintien des capacités d'autonomie des installations, notamment sur les accès contribuant directement à la continuité d'exploitation des bâtiments et à la sécurisation des périmètres sensibles.

* Principes de séparation des alimentations

Afin de garantir la stabilité du système de contrôle d'accès, la résilience des installations et la continuité de fonctionnement des équipements de décision, l'Université impose un principe de séparation fonctionnelle des alimentations.

Les équipements assurant les fonctions de gestion, de décision ou de supervision des accès devront être alimentés indépendamment des équipements de verrouillage.

À ce titre, devront notamment disposer d'une alimentation dédiée :

- les unités de traitement locales (UTL) ;
- les contrôleurs d'accès ;
- les modules d'entrées/sorties ;
- les modules de communication ;
- les interfaces réseau ;
- les équipements participant à la prise de décision ou à la transmission des événements.
- Les équipements de terrain générant des appels de courant importants ou susceptibles de provoquer des perturbations électriques devront être alimentés par des circuits distincts. Ils concernent notamment :
- les ventouses électromagnétiques ;
- les gâches électriques ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- les serrures électromécaniques ;
- les serrures motorisées ;
- les dispositifs de condamnation motorisés ;
- les automatismes d'accès ;
- les équipements de contrôle d'accès véhicules.

Le raccordement d'un dispositif de verrouillage autre que gâche à impulsion, directement sur l'alimentation d'une UTL ou d'un automate de porte ne sera pas admis.

Le titulaire devra veiller à ce que tout défaut affectant un organe de verrouillage, une batterie ou une alimentation terrain ne soit pas susceptible d'entraîner l'arrêt, le redémarrage ou le dysfonctionnement des équipements assurant l'intelligence du système de contrôle d'accès.

Les études et travaux réalisés dans le cadre du marché devront privilégier une architecture permettant :

- l'isolement des défauts ;
- la maintenance indépendante des équipements ;
- la supervision des alimentations ;
- la continuité de fonctionnement des automates en cas de défaillance d'un verrouillage ;
- une meilleure maîtrise des opérations de maintenance et de dépannage.

* *C.5 Patrimoine technique et documentation*

Le maintien en condition opérationnelle couvre également l'ensemble des éléments documentaires nécessaires à l'exploitation, à la maintenance et à la pérennité du système.

À ce titre, le titulaire devra assurer :

- la tenue à jour de l'inventaire des équipements ;
- la mise à jour des DOE ;
- la mise à jour des schémas et synoptiques ;
- la traçabilité des modifications réalisées ;
- le suivi du cycle de vie des équipements ;
- la gestion des références matérielles ;
- le suivi de l'obsolescence des matériels.

* *D. Obligation de conseil*

Compte tenu de la criticité du système de contrôle d'accès pour le fonctionnement de l'Université et de la trajectoire de transformation engagée par l'établissement, le titulaire est soumis à une obligation permanente de conseil, d'alerte et de proposition.
Cette mission constitue une composante essentielle du marché et s'exerce sur l'ensemble des périmètres couverts par ses prestations.

Le titulaire est tenu à une obligation permanente de conseil, d'alerte et d'anticipation. Toute situation présentant un risque pour la disponibilité, la sécurité, la maintenabilité ou la pérennité du système devra faire l'objet d'un signalement formalisé auprès de l'Université.

Le défaut de conseil ou l'absence de signalement d'une situation dont le titulaire avait connaissance ou dont il ne pouvait raisonnablement ignorer l'existence pourra être considéré comme un manquement à ses obligations contractuelles et donner lieu, selon la gravité des faits constatés, à l'application des mesures prévues au CCAP, sans préjudice des responsabilités qui pourraient lui être imputées.

À ce titre, le titulaire devra mettre à profit son expertise afin d'accompagner l'Université dans la maîtrise, l'exploitation et l'évolution de son système de contrôle d'accès.
Le titulaire devra notamment :

- signaler toute situation susceptible d'affecter la disponibilité, la fiabilité ou la sécurité du système ;
- identifier les équipements présentant un risque de défaillance, d'obsolescence ou de rupture de maintenance ;
- alerter l'Université sur toute évolution réglementaire, normative ou technologique susceptible d'avoir un impact sur les installations ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- proposer des actions préventives permettant d'éviter les situations de dégradation ou d'indisponibilité ;
- contribuer à l'amélioration continue des performances et de la maintenabilité du système ;
- participer à la réduction progressive de la dette technique identifiée par les audits ;
- identifier les opportunités d'optimisation technique, économique ou opérationnelle ;
- signaler les incohérences documentaires ou patrimoniales constatées lors des interventions ;
- formuler des recommandations visant à améliorer le niveau de sûreté des bâtiments et des infrastructures ;
- proposer des scénarios d'évolution compatibles avec les orientations techniques retenues par l'Université.

Le titulaire devra porter une vigilance particulière aux infrastructures participant directement :

- à la continuité d'exploitation des bâtiments ;
- à la protection des personnes ;
- à la protection des biens ;
- à la sécurisation des activités de recherche ;
- à la sécurisation des zones sensibles ou réglementées ;
- à la maîtrise des accès véhicules.

Chaque fois qu'une situation à risque est identifiée, le titulaire devra produire une analyse argumentée comportant :

- la description de la situation constatée ;
- l'évaluation des impacts potentiels sur l'exploitation, la sûreté ou la maintenance ;
- le niveau d'urgence associé ;
- les mesures conservatoires éventuellement nécessaires ;
- les préconisations techniques recommandées ;
- une évaluation budgétaire indicative lorsque cela est pertinent.

L'Université attend également du titulaire qu'il contribue activement aux instances de pilotage du marché.
À ce titre, il devra présenter périodiquement une synthèse des risques identifiés, des actions correctives proposées, des opportunités d'amélioration et des recommandations permettant d'éclairer les décisions de la Maîtrise d'Ouvrage. Ces présentations auront lieu de manière trimestrielle.

L'obligation de conseil s'inscrit enfin dans une logique de partenariat avec l'Université et ne saurait être limitée aux seuls équipements couverts par une demande d'intervention.
Le titulaire devra adopter une démarche proactive de surveillance, d'anticipation et d'accompagnement, visant à garantir la pérennité, la résilience et l'évolutivité du système de contrôle d'accès tout au long de la durée du marché.

* *E. Maintenance préventive*

Le titulaire devra mettre en œuvre une maintenance préventive structurée et documentée visant à maintenir les équipements dans un état optimal de fonctionnement.

○ Objectifs de la maintenance préventive

Cette maintenance aura notamment pour objectifs :

- la réduction des incidents ;
- l'amélioration de la disponibilité globale du système ;
- la détection précoce des dysfonctionnements ;
- la prolongation de la durée de vie des équipements ;
- la sécurisation des infrastructures critiques.

Le titulaire établira un programme annuel de maintenance préventive soumis à validation de l'Université.
Chaque intervention donnera lieu à la production d'un rapport détaillé incluant :

- les équipements contrôlés ;
- les anomalies constatées ;
- les actions réalisées ;
- les recommandations associées ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- les éventuelles préconisations de renouvellement.

○ Caractéristiques et périmètre des visites préventives

2 visites préventives seront à programmer sur l'ensemble des portes extérieures. Les portes intérieures seront incluses dans le périmètre de la maintenance corrective.

Ces visites auront lieu sur l'ensemble des portes réparties de la manière suivante :

- La Doua 191
- Gerland 19
- Rockefeller 41
- Observatoire 5
- Les IUT (3 sites) 105
- Lyon Sud 35
- Buire 30

Total => 426 lecteurs concernés dont 44 barrières.

○ Visite de prise en charge

Dans le cadre de la reprise du périmètre de maintenance, le titulaire réalisera une visite de prise en charge exhaustive des installations de contrôle d'accès de l'Université.
Cette visite a pour objectif d'établir l'état initial du patrimoine à la date de démarrage du marché et de disposer d'une référence commune entre l'Université et le titulaire pour le suivi futur des prestations de maintenance, d'exploitation et de renouvellement.
La visite de prise en charge devra être programmée dans un délai maximal d'un mois à compter de la notification du marché. Elle sera réalisée au cours du premier trimestre 2027 et portera sur l'ensemble du périmètre couvert par le présent marché.
Cette prestation comprendra notamment la vérification et la qualification des équipements suivants :

- les 1 637 lecteurs de contrôle d'accès ;
- les 44 barrières de contrôle d'accès véhicules ;
- les unités de traitement locales (89 UTL) et leurs équipements associés ;
- les modules de raccordement et interfaces de communication ;
- les organes de verrouillage ;
- les dispositifs de commande et de détection ;
- les infrastructures de communication de terrain ;
- les alimentations, batteries et équipements de continuité énergétique ;
- l'ensemble des éléments constitutifs du système tels que définis aux paragraphes C.1 à C.4 du présent article.

À l'issue de cette campagne de prise en charge, le titulaire établira un état patrimonial de référence (T0) comprenant notamment :

- la cartographie technique des installations ;
- l'inventaire consolidé des équipements ;
- l'identification des équipements non conformes ou dégradés ;
- les écarts constatés entre les installations et la documentation disponible ;
- les situations d'obsolescence identifiées ;
- les risques susceptibles d'impacter l'exploitation ou la pérennité du système ;
- les recommandations techniques immédiates ou à moyen terme.

La maîtrise des ouvrages vous livrera des plans.
Ce document constituera la référence contractuelle initiale pour le suivi du patrimoine pendant toute la durée du marché. Il sera présenté lors d'une réunion de restitution dédiée et soumis à validation de la Maîtrise d'Ouvrage.

Les anomalies, non-conformités, dégradations ou dysfonctionnements constatés lors de cette visite ne sont pas réputés inclus dans le périmètre de remise en état initial du marché. Ils feront l'objet, le cas échéant, d'une proposition de plan d'action accompagnée des devis correspondants avec validation de la Maîtrise d'Ouvrage.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Le titulaire disposera d'un délai maximal d'un mois à compter de la validation du rapport de prise en charge pour transmettre l'ensemble des chiffrages associés aux actions correctives préconisées.

- Nature et étendue du contrôle

Le titulaire mettra en œuvre une politique de maintenance préventive structurée permettant de garantir le maintien du niveau de performance, de disponibilité et de sûreté des installations couvertes par le marché.
Cette maintenance devra s'appuyer sur les règles de l'art applicables aux systèmes électroniques de sûreté et intégrer les principes issus des **référentiels APSAD** relatifs aux opérations de vérification, d'entretien, de contrôle technique et de traçabilité des installations de contrôle d'accès.

Les opérations réalisées devront permettre de vérifier non seulement le bon fonctionnement des équipements, mais également leur aptitude à assurer durablement les fonctions de sûreté attendues au regard de leur environnement d'exploitation.

Les visites de maintenance devront notamment permettre :

- de vérifier l'intégrité des équipements ;
- de contrôler les performances fonctionnelles des dispositifs ;
- de détecter toute dérive susceptible d'entraîner une dégradation du niveau de sûreté ;
- d'évaluer l'état de vieillissement des composants ;
- d'identifier les situations d'obsolescence ou de fragilité ;
- de vérifier la cohérence entre les équipements installés, leur paramétrage et leur usage réel ;
- de contrôler les dispositifs de secours et de continuité énergétique ;
- de vérifier le maintien des niveaux de sécurité attendus sur les différents périmètres de l'Université.

Chaque visite donnera lieu à un contrôle technique documenté reposant sur une grille de vérification établie par le titulaire et validée par la Maîtrise d'Ouvrage.
Cette grille devra permettre de qualifier l'état de chaque installation selon plusieurs niveaux :

- conforme ;
- conforme avec observation ;
- non conforme ;
- critique.

Les observations et non-conformités identifiées devront être hiérarchisées selon leur impact potentiel sur :

- la continuité de service ;
- la maintenabilité du système ;
- la sécurité des biens et des personnes ;
- le niveau de sûreté du périmètre concerné.

Le titulaire proposera pour chaque non-conformité identifiée :

- une analyse de risque ;
- une mesure conservatoire éventuelle ;
- une recommandation de correction ;
- un niveau de priorité ;
- une estimation budgétaire des travaux nécessaires.

Le titulaire devra formaliser les procédures de contrôle, les grilles de vérification et les critères de qualification des équipements conformément aux principes de traçabilité et de contrôle périodique issus des référentiels APSAD applicables aux systèmes électroniques de sûreté.

D. Maintenance corrective

Le titulaire assurera la prise en charge de l'ensemble des incidents affectant les équipements couverts par le marché.

À cette fin, il mettra à disposition de l'Université une plateforme de gestion des demandes permettant :

- l'enregistrement des incidents ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- le suivi des demandes ;
- la qualification des niveaux de criticité ;
- le suivi des délais contractuels ;
- la consultation des historiques d'intervention ;
- l'émission et le suivi des devis ;
- la mise à disposition des rapports d'intervention.

L'accès à cette plateforme est inclus dans les prestations du marché et doit être mis à disposition de l'ensemble des services autorisés de l'Université.

La plateforme est ouverte 24h / 24, 7 jours sur 7.

Les prestations de maintenance corrective comprennent notamment :

- le diagnostic ;
- l'identification des causes ;
- les mesures conservatoires ;
- la remise en état après validation du devis par l'Université lorsqu'elle est nécessaire ;
- le remplacement des équipements ou composants défaillants ;
- les essais de validation ;
- la remise en exploitation ;
- la mise à jour de la documentation technique si nécessaire.

Une attention particulière sera portée aux équipements assurant la sécurisation :

- des accès principaux des bâtiments ;
- des zones sensibles ;
- des infrastructures techniques critiques ;
- des zones à régime restrictif (ZRR) ;
- des accès véhicules stratégiques.

- Niveaux de criticité

Les incidents sont classés selon les niveaux suivants :

- ✓ **Criticité majeure**

La criticité majeure s'entendra du fait d'un incident impactant :

- une entrée principale de bâtiment ;
- un bâtiment complet ;
- une barrière principale ;
- un périmètre sensible ;
- une ZRR ;
- tout équipement dont l'indisponibilité présente un risque significatif pour la sûreté ou la continuité d'activité.

Engagements minimums :

GTI : 2 heures ouvrées ;
GTR provisoire ou mesure conservatoire : 4 heures ouvrées ;
GTR définitive : selon disponibilité des matériels et validation du devis.

- ✓ **Criticité significative**

La criticité significative s'entendra du fait d'un incident affectant :

- un accès secondaire de bâtiment ;
- plusieurs accès d'une même zone ;
- un équipement de contrôle d'accès fortement utilisé ;
- un équipement dégradant sensiblement l'exploitation sans bloquer totalement l'activité.

Engagements minimums :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

GTI : 4 heures ouvrées ;
GTR : jour ouvré suivant.

✓ **Criticité mineure**

La criticité mineure s'entendra du fait d'un incident n'ayant pas d'impact immédiat sur la sûreté ou l'exploitation générale :

- lecteur isolé ;
- défaut de signalisation ;
- dysfonctionnement partiel ;
- équipement disposant d'une solution de contournement;
- Incident ayant fait l'objet d'une installation provisoire couvrant l'objectif assigné par le dispositif.

Engagements minimums :

GTI : 8 heures ouvrées ;
intervention planifiée sous 5 jours ouvrés maximum.

○ Escalade

En cas d'impossibilité de remise en service immédiate, le titulaire proposera dans les meilleurs délais :

- une mesure conservatoire ;
- une solution de contournement ;
- une estimation du délai de réparation ;
- un plan d'action permettant de maintenir le niveau de sûreté attendu.

A défaut d'une réponse satisfaisante dans le délai de la GTI concerné suivant le niveau de criticité, le soumissionnaire s'expose aux retenues prévues au présent CCTP (voir section jours-amendes).

○ Suivi des performances

Le respect des engagements de GTI et de GTR fera l'objet d'un suivi présenté lors des réunions de pilotage.
Ces dernières sont trimestrielles.
La participation à ces réunions est intégrée dans le chiffrage de service du soumissionnaire.

Les indicateurs suivants seront notamment suivis :

- nombre d'incidents par criticité ;
- respect des GTI ;
- respect des GTR ;
- temps moyen de résolution ;
- incidents récurrents ;
- équipements les plus défaillants ;
- actions correctives proposées.

○ Modalités retenues pour la maintenance corrective

Le titulaire mettra à disposition de l'Université une organisation lui permettant d'assurer les interventions correctives, les mesures conservatoires et les interventions d'urgence nécessaires au maintien en condition opérationnelle du système de contrôle d'accès.

Dans un objectif de simplification administrative et de maîtrise des coûts d'exploitation, les interventions correctives feront l'objet d'un mode de facturation homogène sur l'ensemble de la durée du marché.

✓ Forfait de prise en charge

Toute demande d'intervention validée par l'Université donnera lieu à l'application d'un forfait de prise en charge.

Ce forfait comprend :

- la réception et l'analyse de la demande ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la qualification technique de l'incident ;
- l'organisation de l'intervention ;
- le déplacement du technicien ;
- la première heure de présence sur site ;

Cette heure forfaitaire constitue l'unité minimale de mobilisation du titulaire.

✓ Temps complémentaires d'intervention

Lorsque la durée effective de l'intervention excède l'heure forfaitaire initiale, les prestations supplémentaires seront rémunérées sur la base d'un prix unitaire horaire.

Le temps facturable correspond exclusivement au temps réellement passé sur site à l'exécution des prestations.

Les temps de déplacement supplémentaires ne pourront être facturés en complément de l'heure forfaitaire initiale.

✓ Distinction géographique des interventions

Compte tenu de la répartition géographique du patrimoine de l'Université, deux zones d'intervention sont définies.

- Zone 1 : Sites de l'agglomération lyonnaise

Cette zone comprend notamment :

- Campus de La Doua ;
- Campus Rockefeller ;
- Campus Lyon Sud ;
- Campus de Gerland;
- sites situés dans l'agglomération lyonnaise.

Pour cette zone, le forfait de prise en charge intègre intégralement les frais de déplacement.

- Zone 2 : Sites distants

Cette zone comprend notamment :

- Bourg-en-Bresse ;
- Saint-Étienne ;
- tout autre site situé hors du périmètre métropolitain lyonnais.

Compte tenu des contraintes de déplacement spécifiques associées à ces implantations, le titulaire pourra prévoir un forfait de prise en charge spécifique.
Les modalités financières correspondantes seront précisées au bordereau des prix.

✓ Interventions en astreinte

Le titulaire devra proposer une organisation d'astreinte permettant de traiter les incidents affectant :

- les accès principaux des bâtiments ;
- les bâtiments sensibles ;
- les plateformes techniques ;
- les ZRR ;
- les accès véhicules stratégiques.

Les modalités de déclenchement de l'astreinte ainsi que les conditions financières associées seront définies au marché.
Toute sollicitation de l'astreinte devra être tracée dans l'outil de gestion des incidents.
Tout changement horaire des portes en cas de demande d'astreinte doit être mentionné au niveau de la la DSI.

✓ Transparence des temps d'intervention

Pour chaque intervention, le rapport transmis à l'Université devra mentionner :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la date et l'heure de la demande ;
- la date et l'heure de prise en charge ;
- la date et l'heure d'arrivée sur site ;
- le temps réellement passé ;
- les opérations réalisées ;
- les équipements concernés ;
- la qualification de l'incident ;
- les éventuelles mesures conservatoires mises en œuvre.

Ces interventions font l'objet d'un suivi de la part de la Direction du Patrimoine.

E. Gestion patrimoniale et documentaire

Le maintien en condition opérationnelle comprend également une mission de gestion patrimoniale du système. Le titulaire devra assurer :

- la tenue à jour de l'inventaire des équipements ;
- la mise à jour des DOE ;
- la mise à jour des schémas et synoptiques ;
- la traçabilité des interventions ;
- le suivi des versions logicielles et matérielles ;
- le suivi des garanties.

Un état patrimonial consolidé devra être maintenu pendant toute la durée du marché.

F. Gestion de l'obsolescence

Le titulaire devra assurer une veille permanente sur l'état du patrimoine de contrôle d'accès.
Il produira périodiquement une analyse comprenant :

- les équipements en fin de vie ;
- les matériels non maintenus ;
- les risques de rupture d'approvisionnement ;
- les composants critiques ;
- les préconisations de renouvellement.

Cette analyse devra permettre à l'Université de disposer d'une vision objective de l'évolution de sa dette technique et de planifier les opérations de modernisation nécessaires.

ELEC.12. PRESCRIPTIONS GÉNÉRALES D'INTERVENTION ET D'EXPLOITATION SUR LES SITES DE L'UNIVERSITÉ

A. Objet du chapitre

Le présent chapitre a pour objet de définir les modalités de gestion, d'instruction, de validation et d'exécution des demandes d'évolution du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.

Il vise à garantir que toute création, modification, extension, renouvellement ou adaptation du système soit réalisée dans une logique de cohérence patrimoniale, de maîtrise des coûts d'exploitation, de maintien des niveaux de sûreté et de préservation de la trajectoire technique définie par l'établissement.

Les dispositions du présent chapitre s'appliquent à l'ensemble des opérations réalisées dans le cadre du présent marché, qu'elles concernent :

- des équipements existants ;
- des extensions du patrimoine ;
- des opérations de modernisation ;
- des déploiements spécifiques ;
- des opérations préparatoires à une migration ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- ou des solutions alternatives mises en œuvre sur certains périmètres de l'établissement.

L'objectif recherché est de garantir une évolution maîtrisée du patrimoine de contrôle d'accès tout en préservant les investissements existants, les capacités opérationnelles du système et les exigences de sûreté applicables aux différents bâtiments et activités de l'Université.

B. Horaires d'intervention et continuité d'activité

L'Université est un établissement en activité permanente accueillant quotidiennement des étudiants, enseignants, chercheurs, personnels administratifs, entreprises extérieures et visiteurs.
Le titulaire devra organiser ses interventions de manière à limiter les impacts sur les activités d'enseignement, de recherche et d'administration.
Les interventions seront réalisées, sauf demande contraire de l'Université, durant les horaires habituels d'exploitation des sites.
Toute intervention nécessitant :

- une interruption de service ;
- une coupure d'accès ;
- une neutralisation temporaire d'équipements ;
- une gêne significative pour les usagers ;

devra faire l'objet d'une validation préalable de la Direction du Patrimoine.
L'Université pourra imposer, selon la nature des travaux :

- des interventions hors horaires ouvrés ;
- des interventions en soirée ;
- des interventions durant les périodes de fermeture universitaire ;
- des interventions pendant les congés universitaires.

Le titulaire intégrera ces contraintes dans son organisation et sa planification.

C. Prise en compte des usagers et activités de l'Université

Les prestations sont réalisées dans des bâtiments occupés pouvant accueillir simultanément :

- des étudiants ;
- des personnels administratifs ;
- des enseignants ;
- des chercheurs ;
- des organismes partenaires ;
- des visiteurs ;
- des entreprises extérieures.

Le titulaire prendra toutes les mesures nécessaires afin de limiter :

- les nuisances sonores ;
- les encombrements ;
- les interruptions de circulation ;
- les risques pour les personnes ;
- les perturbations des activités pédagogiques ou scientifiques.

Les zones d'intervention devront être balisées et sécurisées pendant toute la durée des opérations.

L'Université se réserve le droit de suspendre toute intervention dont les modalités seraient jugées incompatibles avec les exigences de sécurité ou de continuité d'exploitation des sites.

D. Gestion des accès, circulation et stationnement

Le titulaire devra respecter les procédures d'accès applicables aux différents sites de l'Université.
Les demandes d'accès devront être réalisées suffisamment en amont afin de permettre l'instruction des autorisations nécessaires.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Le titulaire veillera à ce que son personnel :

- soit identifiable ;
- dispose des autorisations nécessaires ;
- respecte les consignes de sécurité des sites ;
- respecte les règles de circulation et de stationnement en vigueur.

Les interventions ne devront pas perturber :

- les voies de secours ;
- les accès pompiers ;
- les cheminements piétons ;
- les accès aux bâtiments ;

les voies de livraison.

Le stationnement des véhicules de chantier devra être limité aux emplacements autorisés par l'Université.

E. Interventions sur les parkings et accès véhicules

Les interventions réalisées sur les équipements de contrôle d'accès des parcs de stationnement feront l'objet d'une vigilance particulière.
Le titulaire devra maintenir autant que possible :

- la continuité des accès véhicules ;
- les accès des services de secours ;
- les accès des services logistiques ;
- les accès des entreprises autorisées ;
- les accès nécessaires aux activités de recherche et d'enseignement.

Toute indisponibilité prévisible d'une barrière, d'un portail ou d'un dispositif de contrôle d'accès véhicule devra être signalée préalablement à la Direction du Patrimoine et à la Direction Sécurité.
Le titulaire devra proposer, lorsque cela est nécessaire, des mesures compensatoires permettant de garantir la continuité d'exploitation.

A.6 Sécurité des personnels, des usagers et des installations
Le titulaire demeure responsable de la sécurité de son personnel pendant toute la durée de ses interventions.
Il devra prendre toutes les dispositions nécessaires afin de garantir :

- la sécurité des usagers ;
- la protection des biens ;
- la protection des équipements existants ;
- la sécurité de ses personnels ;
- la continuité des dispositifs de sûreté et de sécurité existants.

Toute neutralisation temporaire d'un équipement participant à la sûreté du site devra être portée à la connaissance de l'Université avant son exécution.
Lorsque les travaux conduisent à une dégradation temporaire du niveau de sûreté d'un bâtiment ou d'une zone, le titulaire proposera les mesures conservatoires adaptées.

F. Accès aux zones sensibles

Certaines interventions pourront être réalisées dans :

- des laboratoires ;
- des animaleries ;
- des locaux techniques ;
- des plateformes de recherche ;
- des zones à régime restrictif ;
- des infrastructures critiques.

Le titulaire devra respecter l'ensemble des procédures d'accès applicables à ces zones.
L'Université pourra demander :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la communication préalable de l'identité des intervenants ;
- la justification des habilitations nécessaires ;
- un accompagnement par ses services ;
- la signature de consignes particulières de confidentialité ou de sécurité.

Aucune intervention ne pourra être engagée sans obtention préalable des autorisations requises.

G. Coordination des interventions et coactivité

Les interventions réalisées dans le cadre du présent marché pourront se dérouler simultanément avec :

- des opérations de maintenance ;
- des travaux immobiliers ;
- des opérations techniques pilotées par la Direction du Patrimoine ;
- des interventions liées aux systèmes de sécurité incendie ;
- des opérations de recherche ou d'exploitation spécifiques.

Le titulaire devra intégrer les contraintes de coactivité dans l'organisation de ses interventions.
Il lui appartiendra de prendre connaissance des contraintes existantes, de coordonner ses actions avec les autres intervenants présents sur site et d'appliquer les consignes définies par l'Université.

H. Protection des infrastructures existantes

Le titulaire prendra toutes les dispositions nécessaires afin d'éviter toute dégradation des ouvrages et équipements existants.
Une attention particulière devra être portée :

- aux réseaux électriques ;
- aux réseaux informatiques ;
- aux infrastructures de sûreté ;
- aux installations de sécurité incendie ;
- aux équipements scientifiques ;
- aux installations techniques des bâtiments.

Toute dégradation constatée sera réparée aux frais du titulaire.

I. Continuité des dispositifs de sûreté

Lorsqu'une intervention implique la neutralisation temporaire d'un équipement de contrôle d'accès, le titulaire devra informer préalablement les 3 directions concernées (Direction du Patrimoine, Direction SI et la Direction Sécurité).
Le titulaire proposera systématiquement une mesure compensatoire lorsque l'indisponibilité d'un équipement est susceptible :

- d'affecter la sûreté d'un bâtiment ;
- de compromettre un accès sensible ;
- d'impacter une zone à régime restrictif ;
- de dégrader les conditions d'exploitation d'un site.

L'objectif recherché est de maintenir un niveau de sûreté compatible avec les exigences du bâtiment concerné pendant toute la durée de l'intervention.

J. Gestion documentaire des interventions

Toute intervention devra être tracée.
Le titulaire devra produire :

- un rapport d'intervention sous format numérique, exploitable ;
- les plans mis à jour lorsque cela est nécessaire ;
- les schémas modifiés ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- les références des équipements installés ;
- les essais réalisés ;
- les réserves éventuelles.

Cette documentation devra être intégrée au patrimoine documentaire du système dans le cadre d'une organisation à définir suivant les outils proposés par le soumissionnaire.
Le soumissionnaire proposera la mise à disposition d'un outil partagé permettant l'échange coordonné dans le cadre d'un pilotage de la sûreté et du contrôle d'accès.

K. Contrôles, essais et réception des installations

Toute création, modification, extension ou opération de renouvellement réalisée dans le cadre du présent marché devra faire l'objet des contrôles et essais nécessaires à la vérification du bon fonctionnement des installations avant leur mise en service.

Le titulaire réalisera sous sa responsabilité l'ensemble des autocontrôles permettant de s'assurer :

- de la conformité des équipements installés ;
- de la qualité des raccordements réalisés ;
- du bon fonctionnement des dispositifs de contrôle d'accès ;
- du fonctionnement des équipements de verrouillage ;
- du bon fonctionnement des asservissements ;
- de la cohérence des paramétrages mis en œuvre ;
- de la transmission correcte des informations vers les systèmes concernés.

Les résultats des essais et autocontrôles seront consignés dans un document transmis à la Maîtrise d'Ouvrage préalablement à toute réception.

*K1 - Réception des prestations

Toute opération de création, d'extension ou de modification significative du système de contrôle d'accès fera l'objet d'une réception par la Maîtrise d'Ouvrage.
Cette réception pourra notamment comporter :

- la vérification des équipements installés ;
- le contrôle du fonctionnement des accès ;
- le contrôle des scénarios de fonctionnement ;
- la vérification des asservissements ;
- la vérification des remontées d'information ;
- la vérification des documents remis par le titulaire ;
- la vérification de la mise à jour de l'inventaire patrimonial.

La réception ne pourra être prononcée qu'après remise :

- des rapports d'essais ;
- des documents d'autocontrôle ;
- des plans mis à jour ;
- des schémas modifiés ;
- du DOE lorsque celui-ci est requis ;
- des fiches d'inventaire du matériel installé.

En l'absence de ces éléments, l'Université pourra différer la réception jusqu'à production des documents nécessaires.
La date de réception constituera le point de départ des garanties afférentes aux équipements et prestations concernés.

L. Prescriptions relatives aux infrastructures de câblage

Toute création, extension, modification ou dépose partielle d'une infrastructure de câblage courants faibles devra être réalisée conformément :

- aux normes NF EN 50173, NF EN 50174, ISO/IEC 11801 et à leurs évolutions en vigueur ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- aux réglementations applicables aux Établissements Recevant du Public (ERP) ;
- aux prescriptions des fabricants des câbles, connectiques, baies, chemins de câbles et accessoires ;
- aux exigences de séparation électromagnétique entre réseaux courants forts et courants faibles ;
- aux règles de sécurité incendie applicables au bâtiment concerné.
- Réutilisation des infrastructures existantes

L'entreprise devra privilégier la réutilisation des infrastructures existantes (chemins de câbles, goulottes, fourreaux, réservations, gaines techniques, locaux techniques, etc.) dès lors que :

- leur état mécanique est satisfaisant ;
- leur taux de remplissage reste conforme aux prescriptions normatives ;
- leur capacité permet les extensions prévues ;
- leur conformité réglementaire est maintenue.

Tout constat de non-conformité ou d'insuffisance devra être signalé au maître d'œuvre avant exécution et faire l'objet d'une proposition technique argumentée.

La Maîtrise d'Ouvrage se réserve le droit de retenir un prestataire extérieur pour des prestations connexes (tirage de câbles, ...).

*L1 - Mise en œuvre des cheminements

Les cheminements devront être réalisés de manière à :

- garantir l'accessibilité pour la maintenance future ;
- éviter toute contrainte mécanique sur les câbles ;
- respecter les rayons de courbure imposés par les fabricants ;
- maintenir une séparation permanente avec les réseaux électriques et les sources de perturbations électromagnétiques ;
- assurer la continuité et la protection mécanique des liaisons sur l'ensemble du parcours.

Les câbles ne devront en aucun cas reposer sur les faux plafonds, gaines de ventilation, canalisations ou tout autre équipement technique non prévu à cet effet.

*L2 - Percements et traversées

Les percements, carottages, saignées, réservations et traversées de parois nécessaires à l'exécution des travaux seront à la charge de l'entreprise.

Après passage des réseaux, l'ensemble des traversées de murs, planchers, cloisons coupe-feu et parois techniques devra être reconstitué avec des systèmes de calfeutrement certifiés garantissant :

le degré coupe-feu initial des ouvrages traversés ;
l'étanchéité à l'air et aux fumées lorsqu'elle est requise ;
la conformité aux procès-verbaux et avis techniques applicables.

Les produits de rebouchage et de calfeutrement employés devront être compatibles avec la nature des supports et disposer des certifications réglementaires en vigueur.

*L3 - Identification et repérage

L'ensemble des infrastructures installées ou modifiées devra faire l'objet d'un repérage durable comprenant :

- l'identification des câbles aux deux extrémités ;
- le repérage des chemins de câbles et goulottes ;
- la mise à jour des plans de cheminement et des schémas d'architecture ;
- la fourniture des DOE en fin d'opération.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

M. Respect des référentiels de l'Université

Les prestations réalisées devront être compatibles avec :

- les standards techniques de l'Université ;
- les référentiels de câblage ;
- les référentiels de cybersécurité ;
- les règles patrimoniales ;
- les règles de sûreté applicables aux différents sites.

Le titulaire devra intégrer ces exigences dans l'ensemble de ses propositions techniques.

N. Réversibilité opérationnelle

Tout équipement installé ou modifié devra être documenté de façon à garantir la continuité d'exploitation du système indépendamment de son installateur.
L'Université devra disposer en permanence :

- des schémas ;
- des paramètres ;
- des références ;
- des documentations ;
- des informations nécessaires à la maintenance future.

ELEC.13. GESTION DES DEMANDES, DES EVOLUTIONS ET DES TRAVAUX ANNEXES

A. Principes généraux

Le système de contrôle d'accès constitue un composant stratégique de la politique de sûreté de l'Université. À ce titre, toute évolution du système, qu'elle soit technique, organisationnelle ou fonctionnelle, devra être conduite dans une logique de maîtrise du patrimoine, de cohérence d'architecture et de respect des orientations stratégiques définies par l'établissement.
Les titulaires ne pourront engager aucune évolution du système sans validation préalable suivant les modalités définies au présent article.

Le système de contrôle d'accès de l'Université constitue une infrastructure évolutive dont les besoins peuvent varier selon les sites, les bâtiments, les activités hébergées ou les exigences particulières de sûreté.
Dans ce contexte, l'Université se réserve la possibilité d'adapter localement les solutions mises en œuvre afin de répondre à des besoins spécifiques ou à des contraintes particulières ne pouvant être satisfaits de manière optimale par l'architecture actuellement déployée.

Toute évolution devra toutefois préserver la cohérence globale du système et maintenir les principes de gouvernance définis dans le présent marché.

B. Gestion des demandes d'intervention

Afin de garantir une traçabilité complète des demandes de maintenance et une homogénéité des arbitrages, la Direction du Patrimoine constitue le point d'entrée unique des demandes relatives aux opérations de maintenance du contrôle d'accès.

À ce titre :

- toute demande d'intervention ;
- toute demande de modification ;
- toute demande d'évolution ;

devra être transmise à la Direction du Patrimoine ou validée par celle-ci.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Aucune sollicitation directe des utilisateurs, laboratoires, composantes ou services de l'Université ne pourra donner lieu à une intervention sans validation préalable de la Commission de Contrôle d'accès (voir section E).

Pour la gestion des devis d'installation, l'Université a choisi de confier toutes les orientations à la Commission de Contrôle d'accès (CCA) décrite au point E ci-après.

C. Principes techniques applicables aux diverses évolutions

Toute évolution du système devra être conçue dans un objectif de réutilisation maximale des infrastructures existantes lorsque celles-ci demeurent compatibles avec les besoins exprimés et les règles de l'art.

À ce titre, le titulaire devra privilégier :

- la conservation des infrastructures de câblage existantes ;
- la réutilisation des chemins de câbles existants ;
- la conservation des architectures de communication de terrain ;
- la limitation des travaux de dépose et de reconstruction ;
- la limitation des impacts sur l'exploitation des bâtiments ;
- la réduction des coûts globaux de possession du système.

Les infrastructures de communication courants faibles devront être réalisées conformément aux règles de l'art applicables aux installations de contrôle d'accès, de sûreté et de câblage structuré.
Les câblages nouvellement réalisés devront notamment respecter :

- les exigences applicables aux établissements recevant du public ;
- les prescriptions relatives aux câbles à faibles émissions de fumées et sans halogène ;
- les règles de séparation entre réseaux de courants forts et courants faibles ;
- les exigences de résistance au feu et de calfeutrement des traversées de parois ;
- les normes et réglementations en vigueur à la date d'exécution des travaux.

Toute création ou modification d'installation devra s'accompagner de la mise à jour des plans, schémas, synoptiques, DOE et inventaires du patrimoine.

D. Études préalables

Toute demande d'évolution significative devra faire l'objet d'une étude préalable permettant d'évaluer :

- le besoin fonctionnel exprimé ;
- le niveau de sûreté attendu ;
- les contraintes d'exploitation ;
- les impacts sur le patrimoine existant ;
- les impacts sur les équipes d'exploitation ;
- les impacts budgétaires ;
- les contraintes de cybersécurité ;
- les conditions de maintien dans le temps de la solution envisagée.

E. Gestion des devis

Dans le cadre du présent marché, le titulaire ne pourra transmettre directement à un utilisateur, une composante, un laboratoire ou tout autre service de l'Université aucun devis relatif à la création, l'extension, la modification, le renouvellement ou la suppression d'un équipement de contrôle d'accès sans validation préalable de la **Commission de Contrôle d'Accès de l'Université**.

Cette Commission est composée de représentants des différentes directions concernées par la gouvernance du système de contrôle d'accès.

Tout devis établi devra faire l'objet d'un processus de validation interne visant à garantir la cohérence :

- technique ;
- patrimoniale ;
- fonctionnelle ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- budgétaire ;
- réglementaire ;
- sécuritaire ;

✓ de la demande formulée.

La validation sera réalisée selon les domaines de compétence concernés par le projet :

- Direction du Patrimoine : aspects patrimoniaux, techniques, architecturaux, financiers et travaux ;
- Direction des Systèmes d'Information : impacts logiciels, applicatifs, réseaux, cybersécurité, données, interfaces et systèmes connectés ;
- Direction Sécurité : impacts sur la politique de sûreté, les profils d'accès, les groupes d'autorisation, les périmètres sensibles et les niveaux de sécurité associés.

Le titulaire devra tenir compte de ce processus de validation dans ses délais d'étude, de chiffrage et de réalisation.

Chaque devis devra obligatoirement être accompagné d'une notice technique précisant au minimum :

- l'objet de la demande ;
- le contexte de l'intervention ;
- les équipements existants concernés ;
- les équipements proposés ;
- les incidences fonctionnelles éventuelles ;
- les incidences sur les infrastructures existantes ;
- les impacts sur les systèmes de contrôle d'accès et de supervision ;
- les contraintes de maintenance associées ;
- les éventuelles conséquences en matière de cybersécurité ;
- les hypothèses techniques retenues.

Aucun devis forfaitaire, imprécis ou insuffisamment détaillé ne pourra faire l'objet d'une validation.

L'Université se réserve la possibilité de demander tout complément d'étude ou toute variante technique qu'elle jugera nécessaire avant validation du devis.

F. Présentation et contenu des devis

*F.1 Principes généraux

Toute demande d'évolution, de travaux, de remplacement ou de fourniture donnant lieu à la production d'un devis devra respecter les exigences définies au présent article.

L'objectif poursuivi est de garantir :

- la transparence financière ;
- la traçabilité des demandes ;
- la comparabilité des propositions ;
- la maîtrise des coûts d'exploitation ;
- la bonne application des dispositions du BPU et de la DPGF.
- Les devis devront être suffisamment détaillés pour permettre à l'Université d'apprécier de manière autonome les prestations proposées, les fournitures associées ainsi que les impacts techniques, patrimoniaux et financiers des opérations envisagées.

*F.2 Contenu minimum des devis

Chaque devis devra obligatoirement comporter les éléments suivants :

- le logo et les coordonnées complètes du titulaire ;
- l'adresse électronique dédiée à la réception des commandes ;
- le numéro SIRET de l'entreprise ;
- la désignation du client ;
- le numéro du marché et le numéro du lot concerné ;
- la date d'émission du devis ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- sa durée de validité (minimum 6 mois sauf évolution réglementaire ou variation justifiée des prix) ;
- la description détaillée du besoin ou du dysfonctionnement constaté ;
- le numéro du bon d'intervention ou du compte-rendu associé lorsqu'il existe ;
- le détail des prestations proposées ;
- la référence du BPU utilisée pour chaque fourniture ou prestation ;
- les quantités associées ;
- le prix unitaire ;
- le montant total hors taxes ;
- le montant total toutes taxes comprises ;
- le délai prévisionnel de réalisation à compter de la réception de la commande ;
- la durée prévisionnelle de l'intervention ;
- le nombre d'intervenants prévus.

* F.3 Distinction entre fournitures et main d'œuvre

Les devis devront présenter de manière séparée :
- les fournitures ;
- la main d'œuvre ;
- les prestations spécifiques ;
- les éventuels forfaits applicables.

Aucun coût de main d'œuvre ne devra être intégré au prix des fournitures.
La valorisation des fournitures devra être conforme aux dispositions définies dans le BPU.
La valorisation de la main d'œuvre devra être réalisée à partir des taux horaires ou forfaits prévus au marché.

Un devis type devra être présenté au sein du mémoire technique de l'offre.

* F.4 Prestations sous-traitées

Lorsque tout ou partie de la prestation fait l'objet d'une sous-traitance, le devis du sous-traitant devra être systématiquement joint.

La valorisation sera présentée selon le principe suivant :

Prix sous-traitant × coefficient de majoration défini au BPU = Montant HT présenté à l'Université

Afficher plus de lignes
Le coefficient de majoration ne pourra inclure aucune prestation de main d'œuvre.
Toute prestation de main d'œuvre complémentaire réalisée par le titulaire devra être :
- identifiée distinctement ;
- quantifiée ;
- justifiée ;
- expliquée dans le devis.
- Cette disposition s'applique notamment aux prestations :
- d'accompagnement ;
- de coordination ;
- de supervision ;
- de réception ;
- d'assistance technique.

* F.5 Fournitures non référencées au BPU

Dans le cas où une fourniture ne serait pas présente au bordereau de prix du marché, le devis fournisseur devra être systématiquement annexé à la proposition transmise à l'Université.
La valorisation sera présentée selon le principe suivant :

Prix fournisseur × coefficient de majoration défini au marché = Montant HT présenté à l'Université

Afficher plus de lignes
La main d'œuvre nécessaire à la dépose, à la pose, aux réglages, aux essais et à la remise en service devra apparaître dans une ligne distincte du devis.
Le titulaire devra systématiquement préciser :
- le nombre d'heures ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- la qualification des intervenants ;
- les hypothèses retenues ;
- la justification des temps annoncés.

*F.6 Contrôle et validation

L'Université se réserve la possibilité de demander toute précision complémentaire concernant :

- les temps annoncés ;
- les fournitures proposées ;
- les références utilisées ;
- les conditions de sous-traitance ;
- les coefficients appliqués ;
- les hypothèses techniques retenues.

Tout devis incomplet ou ne respectant pas les dispositions du présent article pourra être retourné au titulaire pour mise en conformité avant instruction.

G. Gestion des demandes d'évolution

Les demandes d'évolution du patrimoine de contrôle d'accès feront l'objet d'une analyse préalable visant à vérifier :

- leur pertinence fonctionnelle ;
- leur cohérence avec l'architecture existante ;
- leur compatibilité avec les orientations techniques du marché ;
- leur impact financier ;
- leur impact sur l'exploitation et la maintenance ;
- leur impact sur les niveaux de sûreté.

Le titulaire devra participer à cette analyse et fournir tous les éléments techniques nécessaires à la prise de décision.

*H. Commission de Contrôle d'Accès

L'Université met en place la Commission de Contrôle d'Accès (CCA) en charge du suivi des évolutions du contrôle d'accès.
Elle associe l'ensemble des composantes de l'Université citées plus haut, impliquées dans la solution de contrôle d'accès.

Cette commission aura notamment pour missions :

- d'examiner les demandes significatives d'évolution ;
- d'arbitrer les demandes de création ou d'extension du système ;
- de veiller à la cohérence globale du patrimoine ;
- de contrôler l'évolution du nombre d'équipements ;
- de limiter la dérive des coûts d'exploitation ;
- de vérifier l'adéquation entre les besoins exprimés et les solutions proposées ;
- de garantir le respect des orientations techniques du présent marché.

Le titulaire pourra être invité à participer à ces réunions afin de présenter ses analyses et ses recommandations.

*I. Modélisation des niveaux de sûreté

Le titulaire devra être en mesure de proposer plusieurs modèles de déploiement en fonction du niveau de sécurité attendu et de la criticité des locaux concernés.

Les solutions proposées devront permettre d'adapter les architectures techniques aux objectifs de sûreté définis par l'Université tout en maintenant une cohérence globale du système.

À titre indicatif, les études pourront être conduites selon plusieurs niveaux de sensibilité :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

* *Niveau 1 – Usage standard*

- ✓ bâtiments d'enseignement ;
- ✓ locaux administratifs ;
- ✓ espaces courants.

* *Niveau 2 – Sensibilité renforcée*

- ✓ laboratoires ;
- ✓ plateformes techniques ;
- ✓ locaux à accès restreint.

* *Niveau 3 – Sensibilité élevée*

- ✓ ZRR ;
- ✓ infrastructures critiques ;
- ✓ locaux présentant des exigences particulières de sûreté ou de traçabilité.

Pour chacun de ces niveaux, le titulaire devra pouvoir proposer :

- une architecture adaptée ;
- les équipements associés ;
- les exigences d'exploitation ;
- les exigences de maintenance ;
- les exigences de continuité de service ;
- les principes de cybersécurité applicables ;
- les impacts financiers et patrimoniaux.

J. Déploiement de solutions spécifiques

L'Université pourra choisir de maintenir l'architecture existante sur la majeure partie de son patrimoine, tout en autorisant, sur certains périmètres préalablement identifiés, le déploiement d'une solution cible tierce. Cette solution devra être compatible avec les environnements concernés et présenter les capacités d'adaptation et d'évolution nécessaires pour répondre aux exigences du référentiel ANSSI applicable.

Le prestataire répondant au lot 1 dans le cadre de la maintenance des équipements, devra également être en mesure de justifier de ses compétences *et* **de ses habilitations, certifications ou qualifications requises pour la conception, l'intégration, le déploiement et la maintenance de la solution préconisée au lot 3.**

Ces périmètres pourront notamment concerner :

- une Zone à Régime Restrictif ;
- un laboratoire sensible ;
- une plateforme technique ;
- un département particulier ;
- un bâtiment isolé ;
- un projet immobilier spécifique ;
- toute infrastructure présentant un niveau d'exigence particulier.

Dans ce cas, les solutions proposées devront démontrer :

- leur pertinence au regard du besoin exprimé ;
- leur compatibilité avec les objectifs de sûreté de l'établissement ;
- leur intégrabilité avec les processus d'exploitation de l'Université ;
- leur capacité à coexister avec les infrastructures actuellement déployées.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

K. Gestion multi-solutions

L'Université n'exclut pas que plusieurs environnements technologiques puissent coexister pendant la durée du marché dans le cadre d'une migration technologique partielle ou totale.

Le titulaire devra donc être en mesure d'intégrer ses prestations dans un contexte pouvant associer :

- la solution historique SIPASS ;
- une solution déployée sur des périmètres spécifiques et qualifiés ;
- des architectures différenciées selon les niveaux de sûreté recherchés.

Le recours à une solution spécifique sur un périmètre donné ne devra cependant pas conduire à une rupture de gouvernance, de documentation, de traçabilité ou de pilotage.

L. Validation des évolutions

Toute création significative d'accès, toute extension du patrimoine ou toute mise en œuvre d'une solution spécifique devra être examinée par la commission de suivi composée :

- de la Direction du Patrimoine ;
- de la Direction des Systèmes d'Information ;
- de la Direction Sécurité.

Cette commission s'assurera notamment :

- de la cohérence avec les orientations techniques du marché ;
- de l'adéquation du besoin ;
- de la soutenabilité de l'exploitation future ;
- de la compatibilité avec les objectifs de sûreté ;
- de l'absence de création de dette technique supplémentaire.

ELEC.14. PRESCRIPTIONS TECHNIQUES APPLICABLES AUX TRAVAUX D'ÉVOLUTION, DE CRÉATION ET DE RENOUVELLEMENT DES INSTALLATIONS DE CONTRÔLE D'ACCÈS

A. Objet du chapitre

Le présent chapitre définit les prescriptions techniques applicables aux opérations de création, d'extension, de modification, de renouvellement et d'amélioration des installations de contrôle d'accès réalisées dans le cadre du présent marché.

Ces prescriptions ont pour objectif :

- d'assurer l'homogénéité des réalisations sur l'ensemble du patrimoine universitaire ;
- de garantir la maintenabilité des installations ;
- de limiter la création de dette technique ;
- de favoriser la réutilisation des infrastructures existantes ;
- d'assurer la compatibilité avec les architectures actuelles et futures du système de contrôle d'accès ;
- de maintenir un niveau élevé de fiabilité, de sécurité et de traçabilité des installations.

Les prescriptions du présent chapitre constituent un socle minimal applicable à l'ensemble des opérations.

B. Principes généraux de conception

Toute évolution du système devra s'appuyer sur les principes suivants :

- recherche systématique de réutilisation des infrastructures existantes ;
- limitation des interventions destructives ;
- standardisation des matériels ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- simplicité d'exploitation ;
- facilité de maintenance ;
- évolutivité des solutions ;
- compatibilité avec les futurs scénarios de migration définis par l'Université.

Le titulaire devra privilégier les architectures permettant une maintenance rapide et une identification aisée des équipements.

C. Prescriptions relatives aux équipements de contrôle d'accès

*C1. Lecteurs

Les lecteurs installés devront permettre la coexistence simultanée de plusieurs générations de badges et de technologies d'identification pendant toute la durée de la trajectoire de modernisation du système de contrôle d'accès, sans nécessiter de remplacement massif des équipements de terrain.

Les lecteurs déployés dans le cadre des opérations d'évolution, de renouvellement ou de création devront être compatibles avec les technologies de badges exploitées par l'Université et permettre l'accompagnement des futures trajectoires d'évolution en matière de sécurité des identités et des accès.

Les lecteurs proposés devront notamment présenter les caractéristiques minimales suivantes :

- fonctionnement sur technologie 13,56 MHz ;
- compatibilité avec les standards ISO 14443 A et B ;
- compatibilité avec les technologies MIFARE Classic, MIFARE Plus, MIFARE DESFire EV2 ou équivalentes ;
- capacité à prendre en charge des identifiants sécurisés utilisant des mécanismes cryptographiques avancés ;
- prise en charge de clés de sécurité individualisées ;
- capacité de lecture multi-technologies permettant d'accompagner les phases de migration des badges existants ;
- possibilité d'exploitation en environnement multi-applicatif ;
- protection des échanges entre le badge et le lecteur contre les mécanismes de clonage les plus courants ;
- support des mécanismes d'authentification mutuelle lorsque ceux-ci sont mis en œuvre par l'Université ;
- mise à jour firmware réalisable sans remplacement systématique du matériel.

Les lecteurs devront également disposer :

- d'indicateurs visuels de fonctionnement ;
- d'une signalisation sonore paramétrable ;
- d'une temporisation de lecture configurable ;
- d'une détection anti-arrachement ou anti-ouverture lorsque cette fonction est disponible ;
- d'une protection contre les perturbations électromagnétiques courantes.

Pour les équipements installés en extérieur ou en environnement exposé, les matériels devront présenter au minimum :

- un indice de protection IP65 ;
- un indice de résistance aux chocs IK08 ;
- une plage de fonctionnement adaptée aux contraintes climatiques locales ;
- une résistance aux rayonnements ultraviolets et aux intempéries.

L'Université privilégiera les lecteurs permettant, sans modification lourde de l'infrastructure, l'évolution progressive vers :

- des identités hautement sécurisées ;
- l'utilisation d'applications mobiles sécurisées ;
- des mécanismes d'authentification renforcée ;
- des environnements nécessitant un niveau élevé de traçabilité ou de sûreté.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Les candidats devront préciser dans leur offre les mécanismes de sécurisation des identifiants, les technologies supportées ainsi que les modalités d'accompagnement des futures migrations technologiques.

* C2. Organes de verrouillage

Les dispositifs de verrouillage devront être adaptés :

- au type de porte ;
- à la fréquence d'utilisation ;
- aux contraintes d'évacuation ;
- aux prescriptions de sécurité incendie.

Le titulaire devra systématiquement vérifier :

- la compatibilité du verrouillage avec l'huisserie ;
- la conformité mécanique du vantail ;
- la qualité des alignements ;
- l'absence d'effort anormal sur les dispositifs installés.

En cela, il devra vérifier :

- la résistance mécanique adaptée ;
- la compatibilité ERP ;
- la compatibilité SSI ;
- le comportement en défaut énergie ;
- le comportement en défaut communication ;
- la durée de vie compatible avec exploitation intensive.

D. Contrôle d'accès sur les portes

Avant toute installation ou modification d'un contrôle d'accès, le titulaire devra vérifier :

- l'état général de la porte ;
- l'état de l'huisserie ;
- le fonctionnement des ferme-portes ;
- la qualité de fermeture ;
- l'absence de déformation susceptible d'altérer le fonctionnement.

Toute anomalie susceptible de compromettre la fiabilité du système devra être signalée à la Maîtrise d'Ouvrage avant réalisation.

E. Équipements minimaux d'une porte contrôlée

Une porte équipée en contrôle d'accès devra intégrer au minimum :

- un lecteur ;
- un dispositif de déverrouillage adapté ;
- un contact de position de porte ;
- un bouton de sortie lorsque requis ;
- les dispositifs de sécurité réglementaires applicables.

Le titulaire devra systématiquement vérifier :

- le temps d'ouverture ;
- le temps de refermeture ;
- la libération des accès en cas de défaut énergie ;
- les interactions avec les dispositifs de sécurité incendie.

F. Alimentation électrique et continuité de service

Toute création ou modification d'installation devra intégrer une analyse de continuité énergétique.

Le titulaire devra :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- vérifier les capacités des alimentations existantes ;
- contrôler les capacités de charge ;
- contrôler les batteries ;
- mesurer les tensions disponibles ;
- vérifier les temps d'autonomie.

Les extensions réalisées ne devront pas conduire à une surcharge des équipements existants.

G. Réseaux de communication et infrastructures de terrain

Le titulaire privilégiera la réutilisation des infrastructures existantes lorsque leur état le permet.

Les nouvelles liaisons devront :

- être clairement identifiées ;
- être repérées aux deux extrémités ;
- être documentées dans les DOE ;
- respecter les règles de séparation des réseaux.

Toute extension de bus RS485 devra faire l'objet d'une étude préalable validant :

- les longueurs cumulées ;
- les conditions de terminaison ;
- les contraintes électromagnétiques ;
- les capacités d'évolution futures.

Les choix techniques de modes de verrouillages sont adaptés aux types de lieux, de contraintes et aux niveaux de sécurité afférents dans le cadre d'une typologie qui peut être décrite de la manière suivante :

- Niveau 1 – usage courant

Ce niveau concerne notamment :

- bureaux ;
- salles d'enseignement ;
- locaux administratifs ;
- salles de réunion ;
- locaux sans enjeu particulier de sûreté.

Les technologies de verrouillage pouvant être mises en œuvre sont notamment :

- gâches électriques ;
- ventouses électromagnétiques ;
- dispositifs équivalents adaptés aux usages courants.

Les solutions retenues devront permettre :

- une exploitation simple ;
- une maintenance réduite ;
- une bonne compatibilité avec les contraintes ERP ;
- un coût global maîtrisé.

- Niveau 2 – Sensibilité renforcée

Ce niveau concerne notamment :

- laboratoires ;
- ateliers ;
- locaux techniques ;
- réserves ;
- espaces à accès restreint ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- locaux présentant un enjeu particulier pour l'exploitation du bâtiment.

Les dispositifs privilégiés sont :

- serrures électromécaniques ;
- serrures motorisées simples ;
- solutions offrant un niveau de résistance supérieur aux dispositifs de niveau 1.

Les équipements devront permettre :

- une meilleure résistance mécanique ;
- une surveillance des états ;
- une traçabilité adaptée ;
- une exploitation intensive lorsque nécessaire.

Niveau 3 – Sensibilité élevée

Ce niveau concerne notamment :

- Zones à Régime Restrictif (ZRR) ;
- infrastructures critiques ;
- laboratoires sensibles ;
- plateformes de recherche à enjeux ;
- locaux nécessitant un haut niveau de protection.

Les solutions de verrouillage pourront notamment s'appuyer sur :

- serrures motorisées haute sécurité ;
- serrures multipoints ;
- serrures trois points motorisées ;
- dispositifs assurant une condamnation renforcée du vantail.

Les solutions devront permettre :

- un niveau élevé de résistance à l'effraction ;
- une supervision complète des états ;
- une traçabilité renforcée ;
- une intégration avec les exigences de sûreté du périmètre concerné.

Choix définitif du niveau

Le niveau de verrouillage retenu sera validé par l'Université au regard :

- de la criticité du local ;
- des exigences de sûreté ;
- des contraintes d'exploitation ;
- des contraintes réglementaires ;
- des objectifs de maintien en condition opérationnelle.

Le titulaire pourra proposer un niveau supérieur lorsqu'il estime que les enjeux de sûreté ou d'exploitation le justifient. Cette proposition devra être argumentée dans le cadre de l'étude préalable et fera l'objet d'une validation de la Direction Sécurité, suivant ses prescriptions initiales.

H. Réalisation des câblages

Les câbles utilisés devront être adaptés aux environnements d'installation.

Les cheminements devront :

- rester accessibles pour la maintenance ;
- être protégés mécaniquement ;
- être repérés ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- respecter les règles de séparation courants forts / courants faibles.

Sauf impossibilité technique dûment justifiée :

- aucun câble ne devra être apparent dans les zones accessibles au public ;
- aucun câblage ne devra être laissé sans protection mécanique ;
- aucun raccord intermédiaire ne devra être réalisé en dehors des coffrets prévus à cet effet.

I. Réception technique des travaux

Toute intervention donnant lieu à une modification fonctionnelle du système fera l'objet d'essais.

Les vérifications minimales comprendront :

- fonctionnement du lecteur ;
- fonctionnement du verrouillage ;
- contrôle des remontées d'information ;
- contrôle des alarmes techniques ;
- contrôle du déverrouillage de sécurité ;
- contrôle des scénarios de secours ;
- cohérence du paramétrage.

Les essais seront consignés dans un procès-verbal transmis à l'Université.

J. Dossier des ouvrages exécutés

Pour toute opération, le titulaire devra remettre un DOE comprenant a minima :

- fiche d'intervention ;
- plans mis à jour ;
- schémas de raccordement ;
- synoptiques modifiés ;
- inventaire du matériel installé ;
- références constructeurs ;
- notices techniques ;
- résultats des essais ;
- paramétrages spécifiques réalisés.
- photographies avant travaux ;
- photographies après travaux ;
- photographies des coffrets modifiés ;
- photographies des raccordements significatifs

L'ensemble des documents devra être fourni sous format numérique exploitable.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

LOT 2 : EXPERTISE FONCTIONNELLE, LOGICIELLE ET GESTION DES DONNEES

ELEC.15. PRINCIPES GENERAUX DE MAITRISE FONCTIONNELLE DE L'ENVIRONNEMENT SIPASS

A. Objet du domaine

Le présent domaine couvre l'ensemble des prestations nécessaires au maintien de la maîtrise fonctionnelle, applicative et opérationnelle du système de contrôle d'accès actuellement exploité par l'Université.

Il porte plus particulièrement sur l'environnement SIPASS, ses mécanismes d'administration, ses interfaces avec le système d'information de l'établissement, ses processus de gestion des habilitations ainsi que la préservation de l'intégrité des données nécessaires au fonctionnement du dispositif de contrôle d'accès.

Les prestations attendues ont pour objectif de garantir la continuité des services actuellement rendus par la plateforme tout au long de la durée du marché, y compris dans les phases d'évolution, de coexistence ou de transformation éventuelle du système. Elle intègre de même la potentielle mise à jour de la solution doublée de la migration serveur afin de corriger une partie de la dette technique identifiée par l'audit mené.

B. Principe de compétence et d'organisation

L'Université considère que la maîtrise de l'environnement SIPASS constitue une compétence critique pour assurer la continuité de fonctionnement du système et sécuriser les trajectoires d'évolution qui pourraient être engagées pendant la durée du marché.

Les études préalables ont démontré que cette compétence est aujourd'hui portée par un nombre limité d'acteurs spécialisés et qu'elle ne constitue pas nécessairement le cœur de métier des intégrateurs intervenant sur les infrastructures physiques de contrôle d'accès.

En conséquence, l'Université n'impose pas que cette expertise soit détenue directement par le titulaire chargé des autres domaines du marché.

En revanche, le candidat devra démontrer sa capacité à mobiliser durablement les compétences nécessaires au maintien, à l'administration et à l'évolution de l'environnement SIPASS.

Cette compétence pourra notamment être apportée :

- par le titulaire lui-même ;
- par un cotraitant ;
- par un partenaire spécialisé ;
- dans le cadre d'un groupement d'entreprises ;
- ou par toute organisation permettant de garantir un niveau d'expertise suffisant pendant toute la durée du marché.

L'Université sera particulièrement attentive à la pérennité de cette organisation et à sa capacité à accompagner les phases de maintien, de coexistence ou de migration éventuelle du système.

C. Mise à niveau de l'environnement SIPASS et sécurisation de l'infrastructure

L'Université considère que la pérennisation temporaire de l'environnement SIPASS constitue un prérequis à toute trajectoire d'évolution du système de contrôle d'accès.

À ce titre, le titulaire devra être en mesure d'accompagner l'Université dans l'analyse, la préparation et la mise en œuvre des opérations nécessaires à la sécurisation et à la modernisation de l'environnement actuellement exploité.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

*C.1 Audit préalable de l'environnement existant

Dans le mois suivant la notification du marché, le titulaire réalisera un audit de l'environnement SIPASS existant portant notamment sur :

- la version logicielle actuellement déployée ;
- l'architecture serveur ;
- les bases de données ;
- les mécanismes de sauvegarde ;
- les interfaces avec le système d'information ;
- les performances générales de la plateforme ;
- les contraintes d'exploitation ;
- les risques techniques et sécuritaires identifiés.

Cette analyse donnera lieu à un rapport de synthèse présentant les opportunités d'évolution, les points de vigilance et les recommandations associées.

*C.2 Mise à niveau de la solution existante

Le titulaire étudiera les conditions permettant une évolution de la plateforme actuelle vers une version plus récente de la solution lorsqu'une telle opération est techniquement réalisable et compatible avec les objectifs de l'Université.

Cette étude devra notamment préciser :

- les prérequis techniques ;
- les impacts sur l'exploitation ;
- les impacts sur les interfaces existantes ;
- les impacts sur les équipements de terrain ;
- les impacts sur la cybersécurité ;
- les conditions de retour arrière ;
- les coûts associés.

Toute opération de mise à niveau fera l'objet d'une validation préalable de l'Université.

*C.3 Modernisation de l'infrastructure serveur

Le titulaire devra être en mesure de proposer les évolutions nécessaires à la sécurisation et à la pérennisation de l'infrastructure hébergeant la plateforme de contrôle d'accès.

Les études réalisées devront notamment intégrer :

- l'évolution des systèmes d'exploitation ;
- l'évolution des bases de données ;
- la stratégie de sauvegarde ;
- la stratégie de restauration ;
- les mécanismes de redondance ;
- les mécanismes de supervision ;
- les exigences de cybersécurité définies par la DSI ;
- les contraintes de continuité de service.

L'objectif poursuivi est de maintenir un niveau de disponibilité compatible avec l'exploitation quotidienne du contrôle d'accès et de réduire les risques associés à l'obsolescence de l'infrastructure, mais aussi, la réduction nette de la mise à jour du référentiel utilisé pour les données dans SiPass.

*C.4 Préparation des futures opérations de migration

Indépendamment des trajectoires qui pourraient être retenues par l'Université, le titulaire devra maintenir la capacité de la plateforme actuelle à participer à d'éventuelles opérations futures de migration technologique.

À ce titre, il devra notamment :

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- maintenir une documentation technique à jour de l'environnement SIPASS ;
- documenter les interfaces existantes ;
- documenter les structures de données utilisées ;
- maintenir les procédures d'export et de reprise des informations ;
- contribuer aux études préparatoires nécessaires à toute évolution future du système de contrôle d'accès de l'Université.
- Cette exigence vise à préserver la capacité de l'Université à faire évoluer son environnement de contrôle d'accès sans dépendance excessive à une technologie ou à un fournisseur particulier.

* *C.5 Coexistence avec une solution cible*

L'Université se réserve la possibilité de déployer, sur certains périmètres ou dans le cadre d'opérations spécifiques, une solution de contrôle d'accès distincte de la plateforme SIPASS actuellement exploitée.

Dans cette hypothèse, le titulaire devra être en mesure d'accompagner les phases de coexistence entre les environnements, notamment en matière :

- d'échange de données ;
- de maintien des habilitations ;
- de cohérence des référentiels ;
- de continuité d'exploitation ;
- de traçabilité des accès ;
- de conservation des historiques.

Les modalités de cette coexistence feront l'objet d'études spécifiques validées par la Direction du Patrimoine, la Direction des Systèmes d'Information et la Direction Sécurité.
Ils auront pour objectif la fluidité dans l'exploitation globale de la solution en vue d'une migration progressive, potentiellement sur plusieurs années.

D. Administration fonctionnelle de la plateforme SIPASS

Le titulaire assurera l'assistance à l'administration fonctionnelle de l'environnement SIPASS actuellement exploité par l'Université.

Cette mission comprend notamment :

- l'administration courante de la plateforme ;
- le maintien des paramétrages existants ;
- l'assistance aux opérations d'exploitation ;
- l'accompagnement des utilisateurs habilités ;
- l'administration des équipements déclarés dans la plateforme ;
- le maintien des mécanismes de supervision et d'exploitation.

L'objectif est de garantir la continuité de fonctionnement de la plateforme pendant toute la durée du marché.

E. Gestion des habilitations et des droits d'accès

Le contrôle d'accès de l'Université repose sur plusieurs dizaines de milliers de porteurs de badges et plusieurs milliers de groupes d'accès.

Le titulaire devra assurer le maintien des mécanismes permettant :

- l'attribution des droits ;
- la modification des droits ;
- la suppression des droits ;
- la gestion des accès temporaires ;
- la gestion des populations particulières ;
- la gestion des accès sensibles.

Le titulaire contribuera à la cohérence globale des habilitations et signalera toute anomalie susceptible d'avoir un impact sur la sûreté ou le fonctionnement du système.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

F. Administration des groupes d'accès

Le titulaire devra assurer une expertise avancée sur la structure des groupes d'accès actuellement exploités dans SIPASS.

Il devra notamment :

- analyser les groupes existants ;
- identifier les incohérences éventuelles ;
- repérer les doublons ;
- identifier les groupes orphelins ;
- proposer des actions de rationalisation.

Toute évolution devra préserver le fonctionnement des processus métiers existants et faire l'objet d'une validation préalable de l'Université, notamment en vue de l'organisation d'une coexistence de solutions pendant une phase de migration progressive pouvant aller jusqu'à plusieurs années.

G. Gestion des référentiels et synchronisations

Le titulaire devra assurer le maintien opérationnel des mécanismes de synchronisation utilisés pour alimenter le système de contrôle d'accès.

À ce titre, il devra maîtriser les interfaces existantes avec :

- SIHAM ;
- APOGEE ;
- UNICAMPUS ;
- le référentiel de personnes exploité par l'Université ;
- les mécanismes d'import et d'export associés.

Le titulaire participera au diagnostic des incidents affectant ces flux et proposera les actions correctives nécessaires lorsque les anomalies concernent le périmètre dont il a la charge.

H. Gestion des populations particulières

Le système de contrôle d'accès de l'Université gère plusieurs types de populations présentant des modalités de gestion différentes.

Le titulaire devra être en mesure d'accompagner l'Université concernant :

- les personnels ;
- les étudiants ;
- les doctorants ;
- les personnels hébergés ;
- les organismes partenaires ;
- les chercheurs associés ;
- les visiteurs ;
- les prestataires.

Une attention particulière devra être portée aux populations ne relevant pas directement des référentiels standards de l'établissement.

I. Qualité, cohérence et audit des données

Le titulaire contribuera à l'amélioration continue de la qualité des données exploitées dans le système.

À ce titre, il devra notamment :

- identifier les anomalies de données ;
- détecter les incohérences de paramétrage ;
- identifier les doublons ;

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

- signaler les données obsolètes ;
- analyser les erreurs d'importation ou de synchronisation.

Un bilan annuel de cohérence des données sera présenté à l'Université dans le cadre des instances de pilotage du marché.
Cette recherche de qualité et de cohérence s'explique par une volonté de rationaliser l'ensemble des informations en vue de l'harmonisation de certains processus.

J. Support expert SIPASS

Le titulaire devra mettre à disposition de l'Université un niveau d'expertise avancé lui permettant de traiter les problématiques complexes liées à l'environnement SIPASS.

Cette expertise devra notamment couvrir :

- l'administration avancée ;
- les mécanismes d'intégration ;
- les analyses de dysfonctionnement ;
- les performances de la plateforme ;
- les problématiques liées aux interfaces ;
- les montées de version ;
- les opérations préparatoires aux migrations futures

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

LOT 3 : EVOLUTIONS ET MIGRATION DE LA SOLUTION EXISTANTE

ELEC.16. PRINCIPES DIRECTEURS D'UNE MIGRATION TECHNOLOGIQUE

A. Objet du domaine

Le présent domaine couvre l'ensemble des prestations d'études, d'ingénierie, de renouvellement, de modernisation et de transformation du système de contrôle d'accès de l'Université Claude Bernard Lyon 1.

Il a pour objet d'accompagner la réduction progressive de la dette technique identifiée lors des audits, d'assurer la pérennité des installations et de préparer les futures évolutions du système de contrôle d'accès dans une logique de maîtrise patrimoniale, de continuité d'exploitation et d'indépendance technologique.

Les prestations de ce domaine ne visent pas à imposer le remplacement systématique des infrastructures existantes mais à permettre leur évolution progressive selon une trajectoire cohérente et soutenable pour l'établissement.

B. Principes directeurs de la trajectoire d'évolution

Les audits, études préalables et essais réalisés par l'Université ont permis d'identifier les forces et les limites de l'architecture actuellement exploitée ainsi que les principaux enjeux associés à son évolution future dans le cadre d'une migration progressive de sa solution.

À la date de rédaction du présent marché, l'Université n'a pas officiellement retenu de solution cible unique destinée à remplacer l'environnement actuellement exploité.

L'établissement ne s'inscrit pas dans une démarche de remplacement intégral et immédiat du système de contrôle d'accès mais dans une logique de transformation progressive, maîtrisée et compatible avec les contraintes d'exploitation d'un patrimoine universitaire de grande dimension dans un contexte de tension financière.

Les candidats devront ainsi intégrer la possibilité :

- du maintien de l'environnement SIPASS sur tout ou partie du patrimoine ;
- de la modernisation progressive de certains composants ;
- de la coexistence de plusieurs architectures ;
- du déploiement de solutions alternatives sur certains périmètres ;
- de migrations partielles ou progressives selon les besoins fonctionnels et sécuritaires de l'établissement.

L'Université sera particulièrement attentive à la capacité des solutions proposées à répondre simultanément aux objectifs suivants :

- réduction de la dette technique identifiée ;
- maintien de la continuité d'exploitation ;
- préservation des infrastructures de terrain existantes lorsque cela est pertinent ;
- amélioration du niveau global de sûreté ;
- maîtrise des coûts d'exploitation futurs ;
- limitation des dépendances technologiques.

C. Rationalisation et maîtrise du nombre d'unités de traitement

Les opérations de renouvellement ou d'évolution du système devront rechercher un équilibre entre les objectifs de résilience, de maintenabilité, de cybersécurité et de maîtrise du patrimoine.

À ce titre, les candidats devront justifier l'organisation retenue pour les unités de traitement, contrôleurs ou équipements assurant les fonctions de décision du contrôle d'accès.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

L'Université n'impose pas de modèle unique de concentration ou de distribution des architectures.

Toutefois, les solutions proposées devront démontrer leur capacité à limiter la multiplication des équipements actifs et à préserver la maîtrise des coûts d'exploitation et de maintenance.

Le remplacement d'une unité de traitement existante par une unité de traitement de nouvelle génération constitue l'hypothèse de référence retenue par l'Université.

Lorsque l'architecture proposée conduit au remplacement d'une unité existante par plusieurs équipements distincts, les candidats devront démontrer les bénéfices apportés par cette approche en matière :

- de résilience ;
- de cybersécurité ;
- de disponibilité ;
- de maintenabilité ;
- d'évolutivité ;
- de coût global de possession.

À titre indicatif, l'Université considère qu'un ratio maximal de remplacement de une unité existante pour trois unités nouvelles constitue une limite raisonnable au regard des objectifs de maîtrise patrimoniale et d'exploitation.

D. Principe d'ouverture et d'interopérabilité

L'Université souhaite privilégier des architectures ouvertes, évolutives et interopérables permettant de conserver durablement la maîtrise de son système de contrôle d'accès.

Les solutions proposées devront démontrer leur capacité à s'intégrer dans un environnement multi-constructeurs et à coexister avec différentes générations d'équipements ou de technologies.
En ce sens, les solutions proposées devront au mieux s'inscrire dans une logique de supervision d'ensemble pour la brique "contrôle d'accès".

Une attention particulière sera donc portée :

- à la disponibilité et à la documentation des interfaces ;
- à la capacité d'échange avec des systèmes tiers et notamment Sipass;
- à la réversibilité des données ;
- à l'indépendance vis-à-vis d'un fournisseur unique ;
- à la possibilité de faire évoluer indépendamment les différentes briques constituant l'architecture globale du système.

Les candidats devront démontrer que les solutions proposées ne conduisent pas à recréer les mécanismes de dépendance technologique identifiés lors des audits réalisés sur le système actuel.

Les études, audits et expérimentations réalisés par l'Université ont permis d'identifier plusieurs caractéristiques considérées comme déterminantes pour les futures évolutions du système de contrôle d'accès.

Sans préjuger du choix définitif d'une solution cible, l'Université sera particulièrement attentive aux architectures permettant :

- la coexistence durable de plusieurs générations de technologies ;
- la préservation des infrastructures de terrain existantes ;
- la réutilisation des réseaux et architectures de communication déployés ;
- la réduction progressive de la dette technique identifiée ;
- la limitation du nombre d'équipements actifs nécessaires à l'exploitation (ratio limite de 3 utl pour 1 remplacée) ;
- l'utilisation d'interfaces ouvertes et documentées ;
- l'interopérabilité avec des équipements de plusieurs constructeurs ;
- l'absence de dépendance excessive vis-à-vis d'un fournisseur unique ;
- la supervision consolidée de l'ensemble du patrimoine de contrôle d'accès ;
- la mise en œuvre progressive de différents niveaux de sûreté adaptés aux enjeux des périmètres concernés.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Les solutions proposées devront démontrer leur capacité à accompagner cette trajectoire sur plusieurs années tout en maintenant la continuité d'exploitation des services existants.

En ce sens, l'Université est à la recherche d'un partenariat stratégique sur plusieurs années.

E. Convergence et supervision des environnements

Quelle que soit la trajectoire retenue, l'Université souhaite conserver une vision consolidée de l'ensemble de son patrimoine de contrôle d'accès.

Les architectures étudiées devront ainsi permettre à terme :

- l'administration cohérente des différents périmètre, voire au mieux la supervision de l'ensemble du parc de contrôle d'accès ;
- la supervision centralisée des événements ;
- l'exploitation homogène des informations de sûreté ;
- la traçabilité des accès ;
- la production d'indicateurs consolidés ;
- le maintien de procédures d'exploitation unifiées.

L'objectif recherché n'est pas la multiplication des systèmes indépendants mais la capacité à fédérer plusieurs architectures autour d'une gouvernance et d'une supervision cohérentes à l'échelle de l'établissement.

L'Université privilégiera les solutions permettant la supervision consolidée de plusieurs environnements de contrôle d'accès au sein d'une même interface d'exploitation.

Cette capacité devra permettre notamment :

- la consultation centralisée des événements ;
- la supervision homogène des accès ;
- la gestion consolidée des alarmes ;
- la production d'indicateurs globaux ;
- l'exploitation simultanée de plusieurs architectures ou technologies.

L'objectif poursuivi est de maintenir une gouvernance unifiée du contrôle d'accès indépendamment de la diversité éventuelle des solutions déployées.

F. Périmètres à sûreté renforcée

L'Université accueille des activités de recherche, des infrastructures techniques et des périmètres présentant des exigences particulières de protection.

Pour ces espaces, l'établissement souhaite pouvoir disposer de solutions permettant une montée en sûreté progressive et adaptée aux enjeux identifiés.

Les architectures proposées devront permettre, lorsque cela est nécessaire :

- le déploiement d'environnements dédiés ;
- l'isolation de certains périmètres ;
- la mise en œuvre de mécanismes de sécurité renforcés ;
- l'application de politiques d'administration adaptées ;
- le maintien d'un niveau élevé de traçabilité et d'auditabilité.

L'Université sera particulièrement attentive aux solutions bénéficiant d'une qualification de sécurité délivrée par l'ANSSI ou engagées dans une démarche active d'obtention de cette qualification pour tout ou partie de leurs composants.

Cette exigence concerne principalement les environnements destinés aux périmètres de recherche sensibles, aux infrastructures critiques et aux zones à régime restrictif.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

G. Compatibilité avec les trajectoires ANSSI et NIS2

L'Université souhaite conserver la possibilité de faire évoluer certains périmètres vers des architectures de sûreté renforcée compatibles avec des environnements qualifiés ou engagés dans une trajectoire de qualification.

Les candidats devront être en mesure de démontrer la capacité de leurs solutions à s'intégrer dans une démarche de sécurisation compatible avec les recommandations de l'ANSSI et avec les exigences de résilience, de gouvernance et de maîtrise des risques issues du cadre NIS2.

L'Université n'envisage toutefois pas l'application uniforme de ces exigences à l'ensemble de son patrimoine.

Une approche différenciée pourra être retenue :

- avec des architectures renforcées pour les zones les plus sensibles ;
- avec le maintien ou l'évolution progressive des infrastructures existantes pour les autres périmètres ;
- avec la coexistence de plusieurs niveaux de sûreté adaptés aux risques réels et aux usages observés.

L'objectif poursuivi par l'Université n'est pas le remplacement d'une technologie par une autre mais la construction progressive d'une architecture ouverte, supervisée, interopérable, évolutive et compatible avec plusieurs niveaux de sûreté, permettant de préserver les investissements réalisés tout en répondant aux enjeux futurs de sécurité, de résilience et de protection des activités de recherche.

H. Maîtrise des coûts récurrents d'exploitation

L'Université porte une attention particulière au coût global de possession des solutions qui pourront être déployées dans le cadre de la trajectoire d'évolution du système de contrôle d'accès.

Les candidats devront intégrer dans leurs analyses non seulement les coûts d'acquisition et de déploiement des solutions proposées, mais également l'ensemble des coûts récurrents induits pendant la durée de vie des systèmes.

Une vigilance particulière sera portée :

- aux coûts de maintenance logicielle ;
- aux coûts de support constructeur ;
- aux coûts de licences ;
- aux coûts de renouvellement des abonnements ;
- aux coûts liés aux environnements de supervision ;
- aux coûts associés aux interfaces et mécanismes d'intégration ;
- aux coûts induits par les évolutions du nombre d'utilisateurs, de badges ou d'équipements.

Les candidats devront clairement identifier les modèles de licence applicables aux solutions proposées et préciser notamment si ceux-ci reposent sur :

- le nombre d'utilisateurs ;
- le nombre de porteurs ;
- le nombre de badges ;
- le nombre d'équipements ;
- le nombre de lecteurs ;
- le nombre de contrôleurs ;
- des mécanismes d'abonnement périodique ;
- ou toute autre métrique susceptible d'entraîner une évolution du coût de possession.

L'Université privilégiera les architectures permettant de maîtriser durablement les coûts récurrents et évitant les mécanismes de croissance automatique des dépenses corrélés à l'évolution naturelle de ses populations ou de son patrimoine.

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION

Compte tenu des volumes actuellement exploités par l'établissement, comprenant plus de 53 000 porteurs et pouvant dépasser 75 000 individus à certaines périodes de l'année, les candidats devront démontrer la soutenabilité économique de leur modèle sur le long terme.

L'Université privilégie les solutions dont le modèle économique est principalement corrélé au patrimoine réellement exploité plutôt qu'au volume des populations gérées, ce dernier étant susceptible d'évoluer significativement au cours de la vie du système.

Les études d'évolution et de migration devront systématiquement présenter :

- ✓ le coût initial du projet ;
- ✓ les coûts annuels récurrents ;
- ✓ les coûts liés aux licences ;
- ✓ les hypothèses d'évolution de ces coûts ;
- ✓ les facteurs de variation associés à la croissance du patrimoine ou du nombre d'utilisateurs.

Les solutions conduisant à une augmentation significative et récurrente des coûts de possession sans bénéfice démontré en matière de sûreté, de résilience ou d'exploitation pourront être considérées comme incompatibles avec les objectifs de maîtrise patrimoniale poursuivis par l'Université.

Le candidat devra démontrer sa capacité à s'inscrire dans une relation partenariale durable avec les constructeurs, éditeurs et fournisseurs nécessaires à la mise en œuvre de la trajectoire retenue par l'Université.

ELEC.17. CONDITION SUSPENSIVE RELATIVE A L'OBTENTION DE FINANCEMENTS SPECIFIQUES AU LOT 3

Pour le présent lot 3, le marché sera notifié sous la condition suspensive suivante de l'obtention des financements nécessaires à la réalisation des prestations objet du marché, à hauteur d'un montant permettant d'assurer leur financement dans les conditions économiques prévues au marché.

La condition suspensive devra être réalisée au plus tard le 31/12/2027

Jusqu'à la réalisation de cette condition, aucune prestation ne pourra débuter et aucun ordre de service, bon de commande permettant le commencement de l'exécution des prestations ne pourra être émis par l'Université. Le titulaire reconnaît avoir été informé, préalablement à la conclusion du marché, du caractère incertain du financement des prestations et accepte que le commencement de l'exécution des prestations soit subordonné à la réalisation de la présente condition suspensive.

En cas de non-réalisation de la condition suspensive à la date précitée, le marché deviendra caduc de plein droit, sans indemnité de quelque nature que ce soit due au titulaire. Aucune prestation ne pourra être exigée du titulaire et aucune indemnisation ne pourra être sollicitée au titre du manque à gagner.

L'Université informera le titulaire, par écrit, de la non-réalisation de la condition suspensive dans les meilleurs délais

FIN DE DOCUMENT

TOUTE REPRODUCTION EST INTERDITELE PRESENT CAHIER DES CLAUSES TECHNIQUES PARTICULIERES A ETE ELABORE AVEC L'ASSISTANCE D'UN AMO. IL NE PEUT ETRE REPRODUIT, DIFFUSE, ADAPTE OU REUTILISE, EN TOUT OU PARTIE, A D'AUTRES FINS QUE CELLES LIEES A LA PRESENTE CONSULTATION ET SANS SON AUTORISATION