

**MISE À DISPOSITION D'UN SYSTÈME DE VOTE
ÉLECTRONIQUE SÉCURISÉ POUR LES ÉLECTIONS
ORGANISÉES PAR L'UNIVERSITÉ SORBONNE NOUVELLE
ET D'UNE EXPERTISE INDÉPENDANTE DU SYSTÈME DE
VOTE ÉLECTRONIQUE.**

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

Référence de la consultation : **USN-VOTEELEC**

Numéro de l'accord-cadre : **2025-033**

*Le présent accord-cadre est passé selon une procédure adaptée en application aux R.2123-1,
R.2162-3 à 5 du code de la commande publique.*

*Son exécution est gérée par bons de commande, en application des articles R2162-13 et R2162-14
du Code de la commande publique.*

Le présent document comprend vingt-deux (22) pages numérotées de 1 à 22

Article 1. Contexte de l'appel d'offres

1.1. Contexte

Depuis avril 2021 et le renouvellement des collèges étudiants aux conseils centraux, l'Université a recours au vote électronique pour la plupart de ses scrutins électoraux. Satisfaite de l'organisation de ces élections et du recours à ce processus, l'Université souhaite poursuivre la dynamique du recours au vote électronique pour ces prochaines élections ; en particulier pour les élections visant au renouvellement complet des conseils centraux de l'Université prévues en avril 2027.

1.2. Enjeux

Les mandats des représentants étudiants (conseils centraux et conseils des structures et composantes d'enseignement) sont renouvelés tous les deux (2) ans.

Les mandats des représentants des personnels (conseils centraux, conseils des structures et composantes d'enseignements) sont renouvelés tous les quatre (4) ans.

Des élections partielles peuvent être organisées en cours de mandat et être plus ou moins importantes en termes de nombre d'électeurs et de scrutins.

1.3. Objectifs

Les objectifs poursuivis par le recours au vote électronique pour les élections de l'université Sorbonne Nouvelle sont les suivants :

Sécuriser et assurer la transparence des opérations de vote

Les moyens pour atteindre cet objectif sont en particulier :

- Recours à une solution éprouvée et respectant de façon démontrable, l'ensemble des préconisations réglementaires (CNIL et Fonction publique) en matière d'élections par internet ;
- Réalisation d'une expertise indépendante ;
- Association des organisations syndicales au processus de sécurité, mise en place d'outils de supervision donnant en particulier aux organisations syndicales, à travers leur participation aux équipes électorales, les moyens de s'assurer à tout moment de l'intégrité des listes électorales et des urnes.
- Protection des données personnelles et des données électorales.

Assurer la facilité d'accès et d'utilisation de l'ensemble des outils mis en œuvre pour le vote

Les moyens pour atteindre cet objectif sont en particulier :

- Fluidité du parcours utilisateur de la mise à disposition des moyens d'authentification jusqu'au vote ;
- Ergonomie et accessibilité (au sens RGAA) de la solution ;
- Utilisation de pictogrammes pour faciliter l'accessibilité de la solution aux publics non francophones ou aux personnes à besoins particuliers ;

- Possibilité d'accéder à la solution en tout lieu (travail, domicile, déplacement, ...) et sur tout support (ordinateur, smartphone, tablette) ;
- Mise à disposition de supports de communication et formation simples pour faciliter l'utilisation de la solution par les électeurs aussi bien que pour les équipes électorales.

Garantir la disponibilité des outils mis en œuvre pour le vote de façon à respecter l'échéance impérative des élections qui sera fixée par décisions ou arrêtés

Les moyens pour atteindre cet objectif sont en particulier :

- Pilotage rigoureux du projet de préparation des outils du vote et des listes électorales ;
- Réalisation d'élections test permettant d'éprouver les outils et les processus ;
- Infrastructures techniques garantissant la performance et la disponibilité des outils pendant toute la période de vote.

Moderniser le processus des opérations électorales

Les moyens pour atteindre cet objectif sont en particulier :

- Réduction au strict minimum de l'utilisation du papier ;
- Réduction de la charge de travail et des coûts pesant sur les services pour la préparation des élections et pour le dépouillement ;
- Mise à disposition rapide des résultats.

Dans ce cadre, il revient aux Titulaires d'exercer leur devoir de conseil pour garantir l'atteinte des objectifs visés ci-dessus.

1.4. Réglementation

La liste suivante n'est pas exhaustive, mais les principales réglementations s'appliquent et se combinent en fonction de la nature de l'élection :

- Code de l'éducation, notamment ses articles L719-1 et suivants relatifs à la composition des conseils, et D719-1 et suivants relatifs aux conditions d'exercice du droit de suffrage et à la composition des collèges électoraux,
- Décret n° 2024-1038 du 6 novembre 2024 relatif aux dispositions réglementaires des livres Ier et II du code général de la fonction publique
- Décret 2020-1205 du 30 septembre 2020 relatif à l'élection ou la désignation des membres du conseil national de l'enseignement supérieur et de la recherche et des conseils des établissements publics d'enseignement supérieur relevant du ministre chargé de l'enseignement supérieur ;
- Délibération n° 2019-053 du 25 avril 2019 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet ;
- Référentiels Généraux en vigueur dans l'administration, notamment le Référentiel Général d'Accessibilité pour les Administrations (RGAA), le Référentiel Général de l'Interopérabilité (RGI) et le référentiel général de sécurité (RGS) ;
- Règlement Général sur la Protection des Données (RGPD) ;
- Statuts de l'Université Sorbonne-Nouvelle, et de ses composantes.

Article 1.5. Définitions

- **Système de vote électronique** : Ensemble des moyens physiques et logiques permettant de mettre en œuvre une procédure de vote électronique
- **Scrutin** : Totalité des votes mis en œuvre sur un même système de vote électronique

Article 2. Objet de l'accord cadre

Le présent accord cadre a pour objet la mise à disposition d'un système de vote électronique sécurisé pour les élections organisées par l'Université Sorbonne Nouvelle et d'une expertise indépendante du système de vote électronique.

Dans la suite du document, l'acronyme SVE désignera la Solution de Vote Électronique / le Système de Vote Électronique recherché(e).

Le présent accord cadre porte sur le vote électronique à l'exclusion de toute autre modalité de vote qui pourrait lui être associée. Il ne porte ainsi ni sur du vote par correspondance, ni sur des machines à voter, ni sur l'organisation de votes à l'urne.

Tous les besoins sont décrits dans le présent Cahier des Clauses Techniques Particulières (CCTP) et dans les documents auxquels il renvoie.

Le présent accord-cadre est composé de deux lots :

- **LOT 1** : Mise à disposition d'un système de vote électronique, organisation et assistance à la conduite des élections
- **LOT 2** : Expertise indépendante du système de vote électronique retenu par l'université Sorbonne Nouvelle

Article 3. Descriptif des élections au sein de l'Université Sorbonne Nouvelle (USN)

3.1 Organisation générale

L'université Sorbonne Nouvelle comprend trois (3) UFR composés de départements selon l'organisation suivante :

- UFR Arts et Médias
 - Département : Cinéma et Audiovisuel (CAV)
 - Département : Institut d'Etudes Théâtrales (IET)
 - Département : Institut de la Communication et des Médias (ICM)

- Département : Médiation Culturelle (MC)
- UFR Littérature, Linguistique, Didactique (LLD)
 - Département : Didactique du Français Langue Etrangère (DFLE)
 - Département : Institut de Linguistique et Phonétique Générales et Appliquées (ILPGA)
 - Département : Littérature et Linguistique Françaises et Latines (LLFL)
 - Département : Littérature Générale et Comparée (LGC)
- UFR Langues, Littératures, Cultures et Sociétés Etrangères (LLCSE)
 - Département : Etudes orientales (EO)
 - Département : Etudes germaniques (EG)
 - Département : Etudes Ibériques et Latino-Américaines (EILA)
 - Département : Etudes Italiennes et Roumaines (EIR)
 - Département : Institut d'Etudes européennes (IEE)
 - Département : Langues Etrangères Appliquées (LEA)
 - Département : Monde anglophone (MA)

L'université comprend deux (2) écoles et instituts au sens de l'article L.713-9 du code de l'éducation :

- L'Ecole Supérieure des Interprètes et des Traducteurs (ESIT)
- L'Institut des Hautes Etudes de l'Amérique latine (IHEAL)

L'Université comprend cinq (5) autres structures d'enseignement

- Service des enseignements en langue (SEL) rattaché à la Direction des études et de la vie universitaire (DEVU)
- Service interdisciplinaire des enseignements mutualisés (SIEM) rattaché à la Direction des études et de la vie universitaire (DEVU)
- Service de la formation continue (SFC) intégré à la Direction de la Formation Tout au Long de la Vie et des relations avec le monde socio-économique (DFTLVIP)
- Service universitaire des activités physiques et sportives (SUAPS)
- Enseignement à distance (EAD)

L'université comprend cinq (5) écoles doctorales :

- ED 120 - Littérature française et comparée
- ED 122 - Europe latine - Amérique latine
- ED 267 - Arts & Médias
- ED 622 - Sciences du langage
- ED 625 - Mondes Anglophones, Germanophones, Indiens, Iraniens et Études Européennes - MAGIE

L'effectif global des étudiants au 01/01/2025 est le suivant : 15624

L'université Sorbonne Nouvelle comprend :

- 1 direction générale des services
- 8 services centraux
- 3 services communs
- 1 service général
- 2 bibliothèques interuniversitaire (Bibliothèque Sainte-Barbe et Bibliothèque Sainte-Geneviève)

L'effectif global des personnels au 01/01/2025 est le suivant : 1517

3.2. Instances à élire

L'université comprend trois (3) conseils centraux :

- Le Conseil d'administration
- La Commission de la Formation et de la vie Universitaire
- La Commission de la Recherche

Chaque UFR, département, école et institut dispose d'un conseil composé de représentants de personnels et de représentants étudiants.

Pour chacune de ces instances, les mandats des étudiants sont renouvelés tous les deux (2) ans et ceux des personnels sont renouvelés tous les quatre (4) ans.

Des élections partielles peuvent intervenir en cours de mandat.

Les élections professionnelles sont organisées tous les quatre ans par l'université, selon un calendrier défini pour l'ensemble de la fonction publique, pour élire les représentants du personnel parmi les listes présentées par les organisations syndicales.

Article 4. Description des prestations du LOT 1 - Mise à disposition d'un système de vote électronique, organisation et assistance à la conduite des élections

4.1. Objet

La solution recherchée, décrite dans le présent CCTP et dans les documents auxquels il renvoie, consiste en :

- La mise à disposition d'un système, sécurisé, hébergé et maintenu de vote électronique à distance *via* internet dont l'accès se fait 24h/24 et 7j/7 pendant la période des élections par le navigateur du votant ou du superviseur, à partir de tout type de terminal (ordinateurs, tablettes et smartphones) connecté à internet. Les exigences techniques et de sécurité sont détaillées dans l'article 4.8;
- La réalisation de paramétrages pour couvrir les besoins spécifiques de l'université Sorbonne Nouvelle ;
- Organisation et assistance à la conduite des élections.

La solution mise à disposition par le Titulaire du lot 1 devra être conforme à l'ensemble des textes juridiques afférents aux élections des représentants des usagers et des personnels au sein de l'Université et devra par ailleurs répondre à l'ensemble des éléments figurant dans le présent CCTP et dans les documents auxquels il renvoie.

Elle devra permettre d'organiser les élections qui découleraient d'une évolution réglementaire ou des conséquences liées à l'annulation d'un ou plusieurs scrutins.

Le système proposé par le candidat doit respecter les principes fondamentaux qui commandent les opérations électorales, notamment :

- La sincérité des opérations électorales,
- L'accès au vote de tous les électeurs,
- Le secret du scrutin,
- Le caractère personnel, libre et anonyme du vote,
- L'intégrité des suffrages exprimés,
- La surveillance effective du scrutin,
- Le contrôle *a posteriori* par le juge de l'élection.

4.2. Décomposition des prestations attendues

Les prestations attendues sont décomposées en 7 volets :

- Volet 1 : lancement du projet, mise en place de l'organisation et des outils de gestion du projet
- Volet 2 : définition du dispositif organisationnel, fonctionnel et technique des élections organisées
- Volet 3 : mise à disposition, paramétrage/adaptation et infogérance de la solution de vote électronique
- Volet 4 : démonstrateur, élections test et contribution à l'expertise indépendante ;
- Volet 5 : formation à l'utilisation de la solution de vote électronique et assistance à la conduite du changement
- Volet 6 : organisation et tenue des élections organisées incluant l'assistance à l'université notamment lors du dépouillement - organisation et tenue des réélections à la suite d'éventuelles annulations
- Volet 6 bis : transmission des moyens de vote
- Volet 7 : assistance utilisateurs

4.3. Délais

Le Titulaire du lot 1 devra être en capacité d'organiser le vote électronique dans un délai de quatre (4) semaines. Ce délai débute à compter de l'envoi du bon de commande par mail + 1 jour au Titulaire pour chaque élection.

4.4. Accompagnement du projet

Le Titulaire du lot 1 accompagne l'Université dans la réalisation des différentes élections prévues dans le cadre de cet accord cadre, non seulement sur un plan logiciel, mais aussi sur l'aspect organisationnel et légal.

L'accompagnement porte sur toutes les phases du projet, y compris sur la détermination du niveau de sécurité du système de vote par électronique mis en place et les mesures de sécurité techniques et fonctionnelles associées.

Le Titulaire du lot 1 désigne un chef de projet spécialisé dans l'organisation d'élections par vote électronique pour assurer le suivi des opérations électorales ainsi qu'un suppléant en cas d'empêchement du chef de projet principal.

Le chef de projet ou son suppléant devront être impérativement présents sur site ou à distance pendant toute la durée des opérations, lors des formations et des opérations de scellement/descellement et de dépouillement des urnes.

4.5. Assistances attendues

4.5.1. Cellule d'assistance technique

Le Titulaire du lot 1 met en place une cellule d'assistance technique pour chaque scrutin ou pour l'ensemble des opérations électorales en cas de renouvellement complet des conseils : elle est chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique et comprend des représentants de l'Université et du Titulaire.

De l'ouverture du scrutin à sa clôture, le Titulaire met à la disposition de l'Université une équipe assurant le bon fonctionnement du système 24 heures / 24, 7 jours / 7.

Cette équipe rend compte de chaque incident et peut être contactée d'urgence en cas de dysfonctionnement du système.

4.5.2. Assistance aux électeurs

Le Titulaire met à la disposition des électeurs une assistance téléphonique accessible pendant toute la durée du scrutin. La plage horaire ne peut être inférieure à 08h-19h du lundi au vendredi.

Le numéro d'appel, gratuit, est indiqué dans les courriers et sur l'écran d'accueil du site de vote.

Une assistance en ligne est également mise en place par le titulaire et reste accessible pendant toute la durée du scrutin. Elle consiste en une page dédiée du site de vote pour que l'électeur puisse en particulier déposer une demande de renvoi de codes, après vérification de l'identité de l'électeur selon tout procédé fiable.

L'électeur doit se voir proposer plusieurs modalités de réexpédition de ses codes.

4.6. Formation des membres du bureau de vote

Le Titulaire du lot 1 assure une formation des membres des bureaux de vote. Les documents de présentation y afférents leur sont communiqués.

4.7. Plateforme de vote électronique

Le Titulaire du lot 1 assure la mise à disposition et l'hébergement d'un système de vote électronique à distance par Internet sécurisé, la préparation, la gestion et du vote électronique, sous contrôle de l'université Sorbonne-Nouvelle.

La solution offre les meilleures prestations de sécurité possibles et est compatible avec la législation en vigueur et les recommandations de la CNIL.

4.7.1. Hébergement du système

Le système de vote électronique n'est pas hébergé par l'université Sorbonne Nouvelle.

Le système de vote est hébergé par un prestataire de services dont l'activité est régie par le droit de l'Union Européenne. Aucun flux d'administration ni de supervision ne doit être situé hors de l'Union Européenne.

Le système doit comporter un dispositif de secours, également localisé sur le territoire national mais sur un site géographique distinct, pour prendre le relais en cas de défaillance du système principal avec des garanties identiques.

Le centre d'hébergement et le centre de secours doivent présenter toutes les garanties de construction, de mesures anti intrusion, anti-feu, etc. et de préférence être conforme aux normes ISO en vigueur ou équivalentes.

Toutes les ressources informatiques constitutives du système informatique sont synchronisées sur une source de temps fiable.

4.7.2. Sécurités du système

Le système proposé dans le cadre du lot 1 doit avoir fait l'objet d'audits récents par des experts indépendants assurant la conformité aux dispositions réglementaires et aux recommandations de la CNIL.

Le système de vote électronique par internet proposé par le candidat doit comporter les mesures physiques et logiques (firewall, cloisonnement, contrôle d'accès aux applicatifs, protection contre les attaques, les intrusions) permettant d'assurer la confidentialité des données transmises, notamment la confidentialité des fichiers constitués pour établir les listes électorales, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

Les algorithmes de chiffrement et de signature électronique, ainsi que les procédés de scellement, devront être réputés « forts » et répondre aux exigences prévues dans le Référentiel Général de Sécurité (RGS), tout en veillant à utiliser strictement des technologies qui répondent aux standards et aux meilleures pratiques actuelles en matière de sécurité.

Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne ne doivent être accessibles qu'aux personnes habilitées.

Le vote électronique par internet doit garantir en toute circonstance la confidentialité et l'anonymat du vote. En aucun cas il ne pourra être possible de croiser la nature du vote et l'identité de l'électeur. Il garantit le chiffrement ininterrompu des bulletins de vote et leur conservation dans un traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs.

Les interventions sur le système de vote doivent être réservées aux seules personnes chargées de la gestion et de la maintenance et ne peuvent avoir lieu qu'en cas de risque d'altération des données. Les bureaux de vote sont immédiatement tenus informés des interventions techniques sur le système de vote ainsi que des mesures prises pour remédier au dysfonctionnement ayant motivé l'intervention.

4.8. Exigences techniques et de sécurité

La solution de vote par internet mise à la disposition de l'Université par le Titulaire doit être accessible par Internet aussi bien depuis un ordinateur, qu'un smartphone ou une tablette, personnel ou professionnel, et être compatible avec la majorité des navigateurs Internet (Internet explorer, Firefox, Safari, Chrome, Opera, Edge, etc.), dans les versions supportées par les éditeurs respectifs quel que soit le type d'équipements, sans nécessiter l'installation de quelque composant ou plugin que ce soit.

La solution de vote par internet doit permettre un fonctionnement avec des navigateurs intégrant les dernières mises à niveau de sécurité. La solution de vote ne doit pas ainsi contraindre l'électeur à revenir à une version ancienne de son navigateur, ni *a fortiori* à une version présentant des failles de sécurité.

La solution de vote doit inclure, pour les postes des électeurs, un outil permettant de diagnostiquer la compatibilité du poste de travail de l'électeur avec les prérequis techniques et, dans le cas d'un diagnostic négatif, elle doit proposer les solutions adéquates : par exemple des liens de téléchargement vers les pages de téléchargement officielles des navigateurs principaux (Firefox, Chrome, Opera, Internet Explorer, Edge, etc.).

La solution de vote ne doit pas nécessiter l'emploi des composants suivants :

- Les plug-ins Adobe (Flash, Acrobat) ;
- Les ActiveX ;
- Les applets Java (JRE) ;

- La suite bureautique Office ni une version donnée d'un logiciel bureautique.

A noter : la lecture des éventuels documents PDF sera déportée sur le lecteur PDF du support utilisé par l'électeur.

L'installation sur le poste de travail de l'administration d'applications tierces par les utilisateurs est interdite. Les applications sont déployées par les administrateurs à travers des mécanismes approuvés.

De plus, la solution doit fonctionner sans nécessiter l'installation d'extensions ou de logiciels non standards du navigateur, ni exiger la modification des paramètres de sécurité par défaut ou des configurations spécifiques du navigateur.

La solution de vote ne doit pas exiger une connexion Internet à haut débit.

La solution de vote par internet propose le protocole TLS, en version 1.3 ou supérieure.

L'utilisation de toute version inférieure (TLS 1.1, TLS1.0, SSLv3, etc.) doit être désactivée.

Les suites cryptographiques sont conformes au RGS. L'accès des utilisateurs aux interfaces Web du système de vote électronique s'effectue avec le protocole *https*.

4.9. Accessibilité

4.9.1. Accessibilité du système

Le vote est accessible aux électeurs 24h/24 durant la période des élections déterminées à partir de n'importe quel terminal connecté à Internet, en se connectant sur le site sécurisé propre aux élections, et ce, quel que soit le système d'exploitation ou le navigateur Internet.

Le système de vote devra être très accessible en offrant des interfaces adaptées à toutes les tailles d'écrans incluant les smartphones et tablettes.

Aucune installation de logiciel sur le poste des électeurs, de plug-in ou d'application mobile ne sera requise pour accéder au site

4.9.2. Accessibilité et non-discrimination

Les services de la solution doivent être :

- Perceptibles : par exemple, faciliter la perception visuelle et auditive du contenu par l'utilisateur ; proposer des équivalents textuels à tout contenu non textuel ; créer un contenu qui puisse être présenté de différentes manières sans perte d'information ni de structure (par exemple avec une mise en page simplifiée) ;

- Utilisables : par exemple, fournir à l'utilisateur des éléments d'orientation pour naviguer, trouver le contenu ; rendre toutes les fonctionnalités accessibles au clavier ; laisser à l'utilisateur suffisamment de temps pour lire et utiliser le contenu ; ne pas concevoir de contenu susceptible de provoquer des crises d'épilepsie ;
- Compréhensibles : par exemple, faire en sorte que les pages fonctionnent de manière prévisible ; aider l'utilisateur à corriger les erreurs de saisie ;
- Robustes : par exemple, optimiser la compatibilité avec les utilisations actuelles et futures, y compris avec les technologies d'assistance ;
- Sans stéréotype de genre : il conviendra de privilégier les mots épicènes (ex : fonctionnaire) et, lorsque cela ne sera pas possible, de recourir aux formes féminines et masculines des mots désignant des personnes (ex : les électrices et les électeurs) ;
- Non-discriminants : il conviendra que la SVE proposée soit accessible à tous et toutes. Son contenu et sa présentation seront exempts de toute forme de discrimination au regard des 25 critères définis par la loi n° 2008-496 du 27 mai 2008.
- La solution de vote électronique doit respecter les critères du WCAG 2.1 (Accessibilité du web) ou être labellisée AccessiWeb au moins au niveau Argent.

4.9.3. Accessibilité des personnels et étudiants malvoyants

La solution de vote électronique doit respecter des normes et standards en matière d'accessibilité.

Un agent ou un étudiant malvoyant ou non-voyant a ainsi la capacité à se connecter et à utiliser les services qui lui sont offerts par ce biais sur le Web.

A cet égard, en conformité avec le référentiel général d'accessibilité pour les administrations (cf. version 4.1.2) il est attendu que la solution respecte les règles d'accessibilité WCAG 2.1, au niveau double A (AA) requis pour les administrations et les services en ligne.

Ce niveau correspond à une labellisation AccessiWeb par l'association BrailleNet de niveau Bronze-Argent. Depuis 2003, BrailleNet a fondé l'écosystème AccessiWeb sur les règles internationales (WCAG) en fournissant un cadre méthodologique et un référentiel technique permettant de vérifier la conformité avec les critères de succès des WCAG 2.0.

Par arrêté du 29 avril 2015, le gouvernement français a officialisé le choix fait par les pouvoirs publics d'adopter le référentiel AccessiWeb HTML5/ARIA comme base du Référentiel Général d'Accessibilité pour les Administrations (RGAA).

4.9.4. Langue

L'interface de la solution de vote électronique est disponible en français.

Il en va de même de l'ensemble des documents disponibles sur l'application de vote électronique.

4.10. Disponibilité et performances attendues des fonctionnalités transactionnelles entre la soumission d'une demande à la solution et l'obtention d'une réponse.

La plateforme doit offrir une qualité de service garantie en termes de tenue de charge.

Un nombre simultané d'électeurs significatif par rapport au nombre total d'électeurs doit être accepté sans dégradation sensible des performances.

Plus précisément :

- La solution permet à 20 000 électeurs de voter sur une période de plusieurs jours lors de plusieurs scrutins simultanés (3 à 20 environ), avec, pour le premier jour et le dernier jour de scrutin des pics de charge prévisibles ;
- La solution permet jusqu'à 20 000 connexions simultanées et jusqu'à 10 000 connexions actives d'électeurs et jusqu'à 1000 connexions actives de membres des bureaux de vote ;
- Pendant toute la durée des scrutins, la solution permet d'enregistrer 500 votes par minute au cours du premier et du dernier jour des scrutins, pendant lesquels des pics de charge sont prévisibles.

L'expression des objectifs de performance des fonctionnalités transactionnelles (traitement transactionnel et traitement décalé) se fera sous la forme de temps de réponse attendus entre la soumission d'une demande à la solution et l'obtention d'une réponse.

4.10.1. Exigences de temps de réponse pour les fonctionnalités transactionnelles

La solution fournira des temps de réponse inférieurs ou égaux aux temps de réponse listés ci-dessous.

| Type de fonctionnalité | Nombre d'accès simultanés | Temps de réponse maximum |
|---|---------------------------|--------------------------|
| Authentification | 5 000 | 5 secondes |
| Affichage des pages accessibles depuis le portail Électeur | 1 000 | 3 secondes |
| Affichage des pages accessibles depuis le portail des bureaux de vote | 500 | 10 secondes |

4.10.2. Exigences pour les fonctionnalités en traitement décalé

La solution sera dimensionnée pour être capable de fournir une réponse dans un délai maximal de 30 minutes, pour les demandes lancées jusqu'à 20 heures, heure de Paris.

C'est notamment le cas de l'export des résultats électoraux au format CSV.

4.10.3. Performance attendue des activités en traitement par lot

La performance attendue concernant les traitements par lots à la charge du Titulaire sont les suivantes :

| Type de fonctionnalité | Volume de données traitées | Temps de réponse maximum |
|---|----------------------------|--------------------------|
| Import et contrôle des listes électorales | 40 000 lignes | 3 heures |

Le Titulaire informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

La disponibilité de la plateforme doit être maximale au niveau matériel, logiciel et réseau pendant la durée des scrutins. La solution de vote électronique doit être accessible 7 jours sur 7, 24 heures sur 24 pendant cette période.

Toute interruption de service doit être limitée à au plus une demi-heure en cours de scrutin. Cette exigence s'applique quelle que soit la nature de l'incident (incident relatif à la sécurité, aux performances, à l'exploitation de la solution ou à ses fonctionnalités).

En revanche, pendant la période pré-électorale, il est admis que des interruptions interviennent dès lors qu'elles sont nécessaires aux mises à jour et maintenances requises et qu'elles ont été planifiées préalablement. La garantie sur le temps de rétablissement (GTR) se situe entre 4 heures et 48 heures.

4.10.4. Continuité d'activité

Le Titulaire s'engage à mettre en œuvre une gestion des risques et des crises. Il est tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art.

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

Outre les aspects de redondance les prestations touchant à la disponibilité comportent *a minima* :

- La sauvegarde des environnements et des données ; au minimum avec une fréquence quotidienne et une rétention de deux semaines
- La restauration des environnements en cas d'incident

- La participation à la définition d'un plan de reprise d'activité (PRA)

Le Titulaire informe préalablement l'Administration de toute opération susceptible de provoquer l'indisponibilité ou une dégradation des performances du système : T0 désignant l'ouverture du scrutin et T1 la clôture du scrutin.

La disponibilité de la plateforme doit être maximale au niveau matériel, logiciel et réseau pendant la période électorale, c'est-à-dire à partir de T0 - 5 jours ouvrés et jusqu'à T1 + 1 jour calendaire. La solution de vote par internet doit être accessible et opérationnelle, sans interruption, 24 heures sur 24 pendant cette période. Toute interruption de service doit être limitée : une (1) à deux (2) heures d'indisponibilité cumulée sont tolérées entre T0 - 5 jours ouvrés et T1 + 1 jour calendaire.

Cette exigence s'applique quelle que soit la nature de l'incident (incident relatif à la sécurité, aux performances, à l'exploitation de la solution ou à ses fonctionnalités). Une page d'information (indiquant la coupure de service) doit être affichée à destination des utilisateurs.

En revanche pendant la période pré-électorale, c'est-à-dire de T0 - 10 jours ouvrés à T0 - 5 jours ouvrés, il est admis que des interruptions interviennent dès lors qu'elles sont nécessaires aux mises à jour et maintenances requises et qu'elles ont été planifiées préalablement. La garantie sur le temps de rétablissement (GTR) se situe entre une (1) heure et quatre (4) heures.

Dans ce contexte, le Titulaire met en place une organisation, des procédures et des moyens matériels et logiciels permettant de détecter rapidement la survenance des incidents, d'assurer la continuité d'activité et si possible, de procéder au retour à un fonctionnement nominal.

Au cours des opérations électorales, la détection des dysfonctionnements doit être immédiate et la bascule sur la plateforme de secours doit être automatique et la reprise doit être effectuée sans délai de remise en fonction des activités. La durée d'indisponibilité maximale admissible (DIMA) est de soixante minutes à deux heures.

Aucune perte de données (PDMA) n'est admise.

Le non-respect de cette obligation constituera un manquement grave aux engagements contractuels du prestataire et donnera lieu, sans préjudice de l'application des dispositions contractuelles applicables en la matière, au paiement de pénalités qui seront dues de plein droit, sans exclure la possibilité pour l'Université de réclamer des dommages et intérêts complémentaires correspondant au préjudice subi.

De plus, le Titulaire met en œuvre une procédure de continuité d'activité basée sur l'utilisation d'au moins deux sites suffisamment distants de sorte qu'un incident majeur se produisant sur l'un d'eux ne perturbe pas le fonctionnement de l'autre. Le Titulaire s'engage à ce que l'hébergement mis à la disposition de l'Université permette de satisfaire les besoins de disponibilité de la solution de vote par internet.

Par ailleurs, il teste régulièrement la procédure de continuité d'activité afin de s'assurer de son efficacité. Il transmet à l'Université les résultats des tests réguliers réalisés sur la plateforme. Il doit également proposer un site de secours, suffisamment distant du site nominal, au cas où ce dernier vient à faire défaut.

Enfin, le Titulaire doit s'assurer que les sauvegardes ne puissent pas être soumises aux mêmes sinistres que la plateforme. Il doit s'assurer que celles-ci sont protégées en intégrité et en confidentialité.

Il est par ailleurs précisé que les performances attendues concernent la plateforme ainsi que la chaîne de liaison dans son intégralité (consultation de la propagande électorale par exemple).

4.10.5. Délais de qualification des incidents et de résolution des anomalies

Le Titulaire met en œuvre une gestion des incidents (au sens ITIL du terme) pour tracer, qualifier, analyser et corriger les dysfonctionnements qui entraînent une indisponibilité de tout ou partie des fonctionnalités voire une altération des performances préjudiciable à l'utilisation de la solution de vote.

A l'usage, on distingue trois niveaux de sévérité de l'incident :

- Bloquant : il empêche la mise en œuvre d'une ou de plusieurs fonctionnalités essentielles de la solution, blocage qui ne peut pas être contourné et nécessite de fait une intervention d'urgence ; par exemple :
 - l'exécution d'un traitement provoque la fermeture intempestive de l'application,
 - la durée excessive d'un traitement consécutif à une action rend l'application inutilisable,
 - un traitement ne conduit à aucun résultat (impossibilité de créer une valeur...);
- Majeur : incident ne touchant pas les fonctionnalités essentielles mais sans solution de contournement pour arriver au résultat attendu ; l'incident ne menace pas l'intégrité des données mais provoque un dysfonctionnement gênant, sans rupture de service; par exemple :
 - valeurs affichées fausses,
 - affichage tronqué des données dans un écran qui empêche la lecture complète du contenu,
 - impossibilité d'imprimer ;
- Mineur : tout autre incident.

Le signalement d'un incident au Titulaire donne lieu à qualification et, selon les cas, à résolution de sa part.

La qualification de l'incident correspond à l'analyse par le Titulaire de la cause de l'incident qui lui est soumis par l'Université. A l'issue de cette analyse, le Titulaire qui assure une assistance de niveau 2 (cf. volet 7) ou le cas échéant de niveau 1, est en mesure de qualifier l'incident en :

- « anomalie », si le dysfonctionnement est avéré et qu'une correction lui incombe

- « erreur d'utilisation », si le comportement du système est lié au fait qu'un utilisateur n'a pas respecté les prérequis techniques, s'il n'a pas suivi la procédure applicative
- « demande d'évolution », si l'incident correspond à un fonctionnement conforme aux spécifications de la solution mais non souhaité par l'utilisateur

La qualification de l'incident peut donner lieu à la communication à l'utilisateur d'une solution de contournement de l'incident signalé.

Qu'elles soient détectées par l'Université ou par le Titulaire, les anomalies seront enregistrées et suivies dans l'outil dédié à cet usage mis en place au moment du lancement du projet.

Le délai de résolution est mesuré entre le moment où le Titulaire reçoit de l'Université la fiche décrivant l'incident et le moment où il a livré la correction dans l'environnement de production.

Ces délais sont définis ci-dessous selon la nature de l'anomalie et la période de survenance de l'anomalie.

| | Pendant l'élection test, durant le mois précédant le vote et dans la semaine suivant la proclamation des résultat | Pendant le vote |
|-----------------|---|---------------------|
| Type d'anomalie | Délai de résolution | Délai de résolution |
| Bloquante | Au plus 2 jours ouvrés | 30 minutes |
| Majeure | Au plus 4 jours ouvrés | 4 heures |
| Mineure | Au plus 8 jours ouvrés | 1 jour ouvré |

La procédure courante de traitement d'une anomalie doit prendre en compte les aspects suivants :

- Analyser la demande de correction et/ou prévention, ses conséquences, décrire les modifications, des ajouts et leurs impacts sur l'existant
- Apporter si nécessaire une solution de contournement aux défaillances constatées, avant correction définitive
- Tenir informée l'Université, dans les différentes instances du projet, de l'avancement du traitement de l'anomalie jusqu'au retour à une situation normale, en respectant les délais liés à la gravité
- Tenir à jour les indicateurs et tableaux de bord de suivi des actions de maintenance qui auront été mis en place au début de la prestation

- Si nécessaire, procéder aux opérations complémentaires nécessaires à la mise en œuvre de la correction afin de remettre le système dans son état nominal de fonctionnement : reprise de données, paramétrage
- Documenter l'ensemble des travaux réalisés
- Réaliser des actions de conseil et d'expertise sur le système ou sur les anomalies identifiées

4.11. Respect des préconisations de la CNIL en matière d'élections par internet

4.11.1. Préconisations CNIL niveau 3

Au regard de la Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment *via* Internet, les objectifs de la CNIL doivent être respectés.

Au regard de ces objectifs de sécurités, quelques éléments importants :

L'intégrité du système et des données du vote doit être garantie et contrôlée en permanence. La liste d'émargement et l'urne électronique doivent faire l'objet d'un procédé garantissant leur intégrité durant le vote, c'est-à-dire assurant qu'ils ne peuvent respectivement être modifiés que par l'ajout d'un bulletin et d'un émargement, dont l'intégrité est assurée, d'un électeur authentifié de manière non-frauduleuse.

Ce procédé doit déceler toute autre modification du système.

En conformité avec les exigences de la CNIL, le système de vote devra donner la possibilité de procéder à des opérations de scellement successives sous la responsabilité des équipes électorales :

- Avant le début du scrutin : scellement des systèmes de vote, de la liste des candidats, de la liste des électeurs
- À la fermeture du vote : scellement de l'urne et de la liste d'émargement
- Après le dépouillement : le système de vote doit être bloqué et les fichiers des logiciels et de données doivent être conservés sous scellés jusqu'à l'épuisement des délais de recours contentieux

Le scellement s'appuie sur « des algorithmes publics réputés forts », de même que le chiffrement de chaque bulletin de vote émis par l'électeur.

Les clés de déchiffrement générées sont confiées publiquement aux équipes électorales.

La vérification des scellements doit pouvoir se faire à tout moment, y compris durant le déroulement du scrutin. Les bureaux de vote doivent disposer d'outils dont l'utilisation ne requiert pas l'intervention du Titulaire pour procéder à la vérification du scellement, par exemple par une prise d'empreinte numérique.

Les solutions de scellement et de chiffrement devront être qualifiées à minima au niveau élémentaire sur la base du RGS V2.

Il est recommandé que les solutions de chiffrement soient qualifiées au niveau standard sur ce même référentiel.

Le système de vote devra assurer une fonction d'horodatage permettant de garantir la date et l'heure et de l'émargement.

L'émargement doit se faire dès la validation du vote de façon à ce qu'un autre vote, pour un scrutin donné, ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés.

4.11.2. Intégrité de l'hébergement

L'ensemble des éléments physiques utilisés pour l'hébergement de la solution doit demeurer intact pendant toute la durée de chaque scrutin, et jusqu'à l'expiration du délai de recours contentieux. En dehors de ces périodes, le Titulaire réduit au minimum indispensable les modifications apportées à la plateforme.

Le Titulaire indique à l'Université au moins une semaine avant la tenue d'un scrutin, toute modification nécessaire de la plateforme d'hébergement, en indiquant toutes les conséquences fonctionnelles et techniques entraînées par la modification.

L'Université estime si la modification décrite nécessite ou non un nouvel audit et une nouvelle recette de la solution.

4.11.3. Intégrité du logiciel

L'ensemble des éléments logiciels constituant le système de vote doit rester intègre depuis sa mise en place pour l'ouverture de la période de vote jusqu'à la fin de la période de recours contentieux du scrutin.

Les éléments logiciels comprennent l'ensemble :

- Des applications composant le système de vote (module d'authentification, module d'émargement, urne électronique, etc.)
- Des systèmes d'exploitation
- Des progiciels sur lesquels les applications sont installées (serveur web, moteur applicatif...) ; et de la configuration de ces éléments

L'intégrité des éléments logiciels signifie que les exécutables, les pages web, les fichiers de configuration ou toute autre partie de l'application n'ont pas été modifiés depuis leur mise en place. Cette intégrité doit pouvoir être prouvée *via* un scellement.

4.11.4. Intégrité des données

Le système de vote doit fournir les moyens de garantir l'intégrité des données qui entrent ou sortent de ce système.

Ainsi, il doit être capable de vérifier l'intégrité des données qui sont insérées dans le système (en vérifiant le scellement) et de sceller des données qui en sont extraites afin que les entités destinataires de ces données puissent elles-mêmes en vérifier l'intégrité.

4.11.5. Traçabilité des accès

Lors du scrutin, tous les accès sur le système de vote doivent être tracés. Cette traçabilité est sécurisée d'une manière qui garantit que les traces des accès sur le système ne peuvent pas être effacées par le Titulaire du système de vote.

Cette traçabilité inclut toutes les opérations effectuées au titre de la gestion des comptes des membres du bureau électoral : créations, modifications, suppressions.

Avant le dépouillement, les traces des accès et de la gestion des comptes sont portées à la connaissance du comité électoral consultatif, dans un format intelligible par un non informaticien.

4.11.6. Traçabilité des traces du système de vote

Les traces du système de vote (module d'authentification, module d'émargement, urne électronique, etc.) doivent être protégées contre toute manipulation, de manière à permettre à l'Université de vérifier leur intégrité et leur authenticité pendant et après la phase de vote.

4.11.7. Protection du système d'authentification

L'authentification des électeurs nécessite la présentation, en plus des codes transmis dans la notice de vote, d'une information personnelle connue de l'électeur.

4.11.8. Nature des mots de passe

La solution inclut une politique de génération des mots de passe destinée à garantir des mots de passe d'une sécurité suffisante : longueur, emploi de différents types de caractères, interdiction des redondances. Leur complexité doit être conforme à la Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017 de 2022.

4.11.9. Protection contre les attaques

La solution comporte un mécanisme pour protéger le système contre les attaques par recherche d'identifiants, de mot de passe (par exemple, délai d'attente incompressible après plusieurs présentations de mots de passe erronés, blocages après plusieurs échecs d'authentification).

4.11.10. Durée des sessions

La solution impose une déconnexion automatique de l'électeur après un certain délai d'inactivité. Ce délai est configurable.

4.11.11. Scellement du dispositif de vote électronique

Toute modification du système de vote doit pouvoir être décelée, de manière à éviter l'exécution durant le scrutin d'un applicatif différent de celui qui aura été audité.

Le contrôle de l'intégrité du système et de sa correspondance avec le système audité doit pouvoir être effectué à tout moment : avant, pendant et à l'issue du scrutin.

La solution inclut les outils et procédures nécessaires à ces vérifications. La formation des membres du bureau électoral (bureau de vote électronique) inclut ces outils et procédures.

4.11.12. Émargement

L'émargement doit se faire dès la validation du vote de façon à ce qu'aucun autre vote ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés.

La liste d'émargement doit être située sur un système distinct de celui contenant l'urne électronique. Cette liste, aux fins de contrôle de l'émargement, ainsi que le compteur des votes ne sont accessibles qu'aux membres du bureau de vote et aux personnes autorisées.

A l'issue du scrutin, la liste d'émargement est enregistrée sur un support scellé, non réinscriptible, rendant ainsi son contenu inaltérable et probant.

4.11.13. Blocage du système après le dépouillement

Le système de vote électronique doit être bloqué après le dépouillement de sorte qu'il soit impossible de reprendre ou de modifier les résultats après la décision de clôture du dépouillement prise par le comité électoral consultatif.

4.11.14. Nouveau processus électoral en cas d'une éventuelle invalidation ou annulation d'une élection

Si cette invalidation ou annulation est la conséquence de la défaillance avérée de la plateforme de vote et donc de la responsabilité du Titulaire, la tenue de la nouvelle élection est à sa charge.

Si cette invalidation ou annulation n'est pas la conséquence de la défaillance avérée de la plateforme de vote, le pouvoir adjudicateur passe un nouveau bon de commande afin d'organiser la ou les nouvelles élections.

Article 5. Nature des prestations du LOT 2 - Expertise indépendante du système de vote électronique retenu par l'université)

5.1. Objet

Préalablement à la mise en place ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des objectifs de sécurité et de confidentialité du système de vote, tels que décrits à l'article 4 du présent CCTP.

Cette expertise est effectuée sous la responsabilité d'un expert du domaine, indépendant, mandaté par l'Université dans le cadre de l'attribution de ce lot.

5.2. Délais

Le Titulaire du lot 2 devra être en capacité d'organiser l'expertise d'un vote électronique dans un délai de quatre (4) semaines. Ce délai débute à compter de l'envoi du bon de commande par mail + 1 jour au Titulaire pour chaque élection.

5.3. Confidentialité

Le Titulaire du lot 2 ayant accès à des informations sensibles, il est tenu de prendre toutes dispositions afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire

5.4. Désignation d'un référent

A compter de la notification de l'acceptation du devis, le Titulaire devra dans un délai de cinq (5) jours ouvrés désigner un référent et un référent suppléant chargés de conduire spécifiquement l'expertise et d'accompagner l'établissement.

La personne désignée devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité
- Ne pas avoir d'intérêt dans la société qui a créé la solution de vote à expertiser, ni au sein de l'université Sorbonne Nouvelle
- Posséder une expérience dans l'analyse des systèmes de vote par correspondance électronique.

5.5. Prestations

5.5.1. Expertise

Le Titulaire du lot 2 devra, préalablement à la mise en place ou à toute modification substantielle de la conception du système de vote électronique, procéder à une expertise indépendante dudit système. L'audit réalisé portera sur la solution de vote et ses conditions de mise en œuvre, en se fondant sur les référentiels et les dispositifs réglementaires (cf article 4).

L'expertise doit couvrir l'intégralité du dispositif :

- Avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement
- Durant le scrutin (utilisation du système de vote)
- Après le scrutin (dépouillement, archivage, etc.)

L'expertise doit notamment porter sur :

- Le code source correspondant à la version du logiciel effectivement mise en œuvre
- Les mécanismes de scellement utilisés aux différentes étapes du scrutin
- Le système informatique sur lequel le vote va se dérouler
- Les échanges réseau
- Les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote
- Les mécanismes d'authentification des électeurs et la transmission des codes à ces derniers
- L'évaluation du niveau de risque du scrutin
- La pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité
- La réalisation de tests d'intrusions, permettant d'apprécier la robustesse
- L'existence de postes dédiés

Cette expertise du système donnera lieu à un rapport d'expertise qui sera remis au responsable de traitement et au prestataire. La méthode et les moyens permettant d'effectuer la vérification du système doivent être décrits dans le rapport d'expertise.

5.5.2. Avis et assistance

- **Fourniture d'un avis préalable à la réunion de scellement des urnes**

Le Titulaire du lot 2 fournit après expertise un avis technique sur la conformité (et une présentation des éventuelles non conformités avec les risques et recommandations associées) une (1) semaine avant la date prévue pour le scellement. Si un élément de non-conformité est détecté, le Titulaire en informe immédiatement l'Université, afin que soit envisagée la mise en place d'une correction.

L'avis sera diffusé aux membres du bureau de vote et il pourra être demandé au Titulaire de présenter les résultats de son expertise à distance ou en présence.

- **Fourniture d'un avis préalable à la réunion de dépouillement**

Le Titulaire fournit un avis technique sur le déroulement réel du scrutin. Cet avis est communiqué avant la réunion de dépouillement. L'avis sera diffusé aux membres du bureau de vote et il pourra être demandé au Titulaire de présenter les résultats de son expertise à distance ou en présence.

- **En cas de contentieux, aide à la rédaction des réponses aux questions portant sur le domaine de l'expertise**

- **Prestations supplémentaires à la demande de l'Université**

Le candidat indique dans le bordereau de prix unitaire les éléments facultatifs suivants, qui seront ou non choisis par l'Université en fonction du niveau du scrutin :

- Assister l'établissement sur la question du choix du niveau de risque du scrutin ;
- Assister l'établissement sur le choix des modalités d'authentification des électeurs ;
- Assistance et présence physique ou à distance lors de la réunion de scellement des urnes et lors de la séance de clôture du scrutin

5.6. Exigences réglementaires générales

Les exigences indiquées dans cette section s'imposent au Titulaire du lot 2 sur tout le périmètre et toute la durée des prestations.

5.6.1. Exigences juridiques

Protection des données et respect des recommandations de la CNIL

Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique

RGPD

Le système et les traitements effectués sur les données nominatives doivent être conformes à la réglementation en matière de protection des données, et notamment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD, règlement général sur la protection des données).

Si le Titulaire entend faire appel à de la sous-traitance, il doit être en mesure de prouver que les exigences liées à la sécurité des données et des traitements, au RGPD et à l'immunité contre toute réglementation extracommunautaire sont respectées par ses sous- traitants.

Le Dossier de consultation comprend notamment l'annexe Clause RGPD.

5.6.2. Concession de droit d'usage du système de vote

L'organisation de chaque scrutin emporte concession du droit d'usage de la solution de vote pour ce scrutin.

5.6.3. Compatibilité RGS/RGI/RGAA

La solution d'un système de vote recherchée doit être compatible avec les Référentiels Généraux en vigueur dans l'administration.

La solution et la plateforme qui l'héberge devront être conformes au RGS (Référentiel Général de Sécurité). Les solutions cryptographiques utilisées devront être qualifiées à minima au niveau élémentaire ; un chiffrement qualifié standard est recommandé et sera évalué en termes de notation technique.

La solution devra se conformer au Référentiel Général d'Accessibilité pour les Administrations (RGAA) et au Référentiel Général de l'Interopérabilité (RGI).

Article 6. Devoir de conseil et de rationalisation

Il est rappelé aux Titulaires de chacun des lots de l'accord-cadre, qu'ils leur incombent un devoir de conseil auprès de l'administration qu'il s'agisse de la solution mise en œuvre, de l'organisation du déroulé des opérations électorales et des prestations de contrôle utilisant la solution, ou encore du projet d'ensemble de préparation de ces élections.

Le Titulaire de chacun des lots a l'obligation de proposer le groupement de certaines prestations si cela est techniquement possible dans un objectif de réduction des coûts pour les bénéficiaires.

Article 7. Confidentialité

Le Titulaire de chacun des lots se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées par la personne publique.

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser la notice de vote et de réaliser les émargements, ainsi que les informations nominatives des membres de l'équipe électorale recueillies aux fins de création de leurs comptes sur la solution de vote, ne peuvent être utilisés qu'aux fins du vote décrites dans le présent CCTP et ne peuvent être divulgués sous peine des sanctions pénales encourues au titre des articles pertinents du code pénal.

L'ensemble des données relatives aux scrutins (les clés de chiffrement/déchiffrement et le contenu de l'urne, des listes d'émargement, des résultats, les liste des opérations effectuées sur la plate-forme, etc.) gérées par la solution de vote et/ou conservées à l'issue du vote sont la propriété de l'université et doivent faire l'objet d'un traitement garantissant leur confidentialité.

La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.

Le Titulaire de chacun des lots s'engage à respecter une clause de confidentialité et de sécurité et à fournir le descriptif détaillé du dispositif technique mis en œuvre pour assurer cette confidentialité. Il fait en sorte que l'ensemble de ses sous- traitants s'engagent dans les mêmes conditions de confidentialité et de sécurité.