

MARCHE PUBLIC TECHNIQUES DE L'INFORMATION
ET COMMUNICATION



UNIVERSITE DE POITIERS
Direction de la commande et de l'achats publics
15 rue de l'Hôtel Dieu 86073 POITIERS CEDEX 9
Tél: 05 49 45 30 65

MISE A DISPOSITION D'UNE SOLUTION DE VOTE DEMATERIALISEE PAR
INTERNET, PRESTATIONS ASSOCIEES ET D'UNE EXPERTISE INDEPENDANTE DU
SYSTEME DE VOTE ELECTRONIQUE POUR LES SCRUTINS ORGANISES PAR
L'UNIVERSITE DE POITIERS

MARCHE N° 2026F002

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

I. Objet

Fondée en 1431, l'université de Poitiers (ci-après « l'Université ») est une des plus anciennes universités d'Europe. L'université de Poitiers est un établissement public à caractère scientifique, culturel et professionnel depuis décret n°84-723 du 17 juillet 1984. Sa communauté comprend approximativement

34 000 étudiants et 3 000 personnels dont 1 400 enseignants-chercheurs et enseignants et 1 600 personnels administratifs et techniques, répartis sur 14 composantes, 22 unités de recherche propres à l'université et de multiples services d'appui. Dotée de la personnalité morale et de l'autonomie pédagogique, scientifique, administrative et financière, elle est gérée de façon démocratique avec le concours de l'ensemble des personnels, des étudiants et de personnalités extérieures. L'Université exerce ses missions de service public de l'enseignement supérieur, de recherche et de diffusion des connaissances et contribue par ses actions aux objectifs ainsi assignés au service public.

Les dispositions du présent Cahier des Clauses Techniques Particulières (CCTP) concernent la mise à disposition d'un système de vote dématérialisé par internet ainsi que les services associés nécessaires à l'organisation des élections permettant d'élire :

1. Les représentants élus aux conseils centraux de l'université de Poitiers :

- a. Conseil d'administration (CA) ;
- b. Commission de la recherche (CR) ;
- c. Commission de la formation et de la vie universitaire (CFVU) ;

2°. Les représentants élus aux conseils des composantes de l'université de Poitiers suivantes :

- a. École Nationale Supérieure d'Ingénieurs de Poitiers (ENSI) ;
- b. Faculté de Droit et Sciences Sociales (UFR Droit) ;
- c. Faculté de Lettres et Langues (UFR Lettres et Langues) ;
- d. Faculté de Médecine et Pharmacie (UFR Médecine et Pharmacie) ;
- e. Faculté de Sciences Économiques (UFR Sciences Économiques) ;
- f. Faculté des Sciences et du Sport (UFR Sciences et du Sport) ;
- g. Faculté des Sciences Fondamentales Appliquées (UFR SFA) ;
- h. Faculté des Sciences Humaines et Arts (UFR SHA) ;
- i. Institut d'Administration des Entreprises (IAE) ;
- j. Institut de Préparation à l'administration générale (IPAG) ;
- k. Institut des risques industriels, assurantiels et financiers (IRIAF) ;
- l. Institut national supérieur du professorat et de l'éducation (INSPE) ;
- m. Institut Universitaire de technologie d'Angoulême (IUT 16) ;
- n. Institut Universitaire de technologie de Poitiers-Niort-Châtellerauld (IUT 86) ;
- o. European interdisciplinary institute (E2i) ;

3°. Les représentants élus de toutes les instances représentatives du personnel de l'université de Poitiers (CSA ; CPE ; CCPANT...) ;

4°. Les représentants des personnels aux conseils des services communs et généraux de l'université de Poitiers, lorsque ces conseils en comportent ;

- a. Service de santé universitaire (SSU) ;
- b. Service commun de documentation (SCD) ;
- c. Entre autres

5°. Les représentants élus aux commissions d'expertise scientifique de l'université de Poitiers ;

6°. Les représentants élus aux conseils des unités de recherche de l'université de Poitiers suivantes :

- a. Laboratoire LITEC
- b. Laboratoire MOVE
- c. Laboratoire PRETI
- d. Laboratoire PRODICET
- e. Laboratoire HERMA
- f. Laboratoire FORELLIS
- g. Laboratoire MIMMOC
- h. Laboratoire RURALITES
- i. Laboratoire MAPP

- j. Laboratoire TECHNE
 - k. Laboratoire IDP
 - l. Laboratoire ISCRIM
 - m. Laboratoire ERDP
 - n. Laboratoire IHD
 - o. Laboratoire CECOJI-UP
 - p. Laboratoire CRIEF
 - q. Laboratoire CEREGE
 - r. Tout autre laboratoire qui pourra être créé au sein de l'Université
- 7°. Les représentants élus aux conseils des écoles doctorales de l'université de Poitiers suivantes :
- a. ED Humanités
 - b. ED Rosalind Franklin
 - c. ED MIMME
 - d. ED Humains en société
 - e. ED Droit et Sciences Politiques « Pierre Couvrat »
 - f. Toute autre école qui pourra être créé au sein de l'Université

Les sièges potentiellement soumis au vote au sein de ces instances, ainsi que la durée des mandats correspondants sont fixés par les textes de référence cités au II du présent document. Cette liste n'est toutefois pas exhaustive et pourra être complétée en fonction des besoins de l'université de Poitiers.

Le système de vote peut éventuellement prendre en charge l'adoption de délibérations par ces instances lorsqu'elles fonctionnent à distance afin de préserver le secret du vote.

II. Textes de références

Le système de vote dématérialisé par internet (Lot n°1) et son expertise indépendante (Lot n°2) doivent impérativement obéir aux normes en vigueur, notamment celles fixées par les textes énumérés ci-dessous :

- 1°. Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit règlement général sur la protection des données (dit « RGPD ») ;
- 2°. Le code de l'éducation ;
- 3°. Le code général de la fonction publique ;
- 4°. La loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;
- 5°. La loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- 6°. L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- 7°. L'ordonnance n° 2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial ;
- 8°. Le décret n° 82-451 du 28 mai 1982 relatif aux commissions administratives paritaires ;
- 9°. Le décret n° 86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'Etat ;
- 10°. Le décret n°99-272 du 6 avril 1999 relatif aux CPE des établissements d'enseignement supérieur ;
- 11°. Le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

- 12°.Le décret n° 2011-184 du 15 février 2011 relatif aux comités techniques dans les administrations et les établissements publics de l'État ;
- 13°.Le décret n° 2011-595 du 26 mai 2011 relatif conditions et modalités de mise en œuvre du vote électronique par internet pour l'élection des représentants du personnel au sein des instances de représentation du personnel de la fonction publique de l'État ;
- 14°.Le décret n° 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 ;
- 15°.Le décret n° 2020-1427 du 20 novembre 2020 relatif aux comités sociaux d'administration dans les administrations et les établissements publics de l'Etat ;
- 16°.L'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité (ci-après « RGS ») et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;
- 17°.L'arrêté du 10 juin 2015 prorogeant les délais de mise en œuvre du référentiel général de sécurité ;
- 18°.La délibération de la Commission nationale de l'informatique et des libertés (ci-après « CNIL ») 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 et son rectificatif ;
- 19°.Les statuts de l'université de Poitiers ;
- 20°.La décision-cadre permanente relative aux modalités de scrutin par voie électronique pour les élections à l'université de Poitiers ;
- 21°.Le règlement intérieur de l'université de Poitiers ;
- 22°.Les statuts et règlements intérieurs des composantes et des services communs et généraux de l'Université de Poitiers ;
- 23°.Le règlement intérieur des Commissions d'expertise scientifique de l'université de Poitiers ;
- 24°.Le règlement général des unités de recherche de l'université de Poitiers et les règlements particuliers de ces unités.

A minima, le système de vote dématérialisé par internet (Lot n°1) et son expertise indépendante (Lot n°2) doivent suivre les évolutions des textes précités, ainsi que, plus globalement, de tout nouveau texte encadrant cette modalité d'expression.

III. Généralités sur le vote électronique à l'Université de Poitiers

L'Université de Poitiers (ci-après l'Université) est un établissement public à caractère scientifique, culturel et professionnel, créé par décret n°84-723 du 17 juillet 1984. Elle est dotée de la personnalité morale et de l'autonomie pédagogique, scientifique, administrative et financière, elle est gérée de façon démocratique avec le concours de l'ensemble des personnels, des étudiants et de personnalités extérieures. L'Université exerce ses missions de service public de l'enseignement supérieur, de recherche et de diffusion des connaissances et contribue par ses actions aux objectifs ainsi assignés au service public.

La mise en œuvre du vote électronique au sein de l'Université vise à :

- 1°. Simplifier et sécuriser l'organisation du processus électoral,
- 2°. Faciliter le vote pour les personnels et/ou usagers en mission ou en déplacement,
- 3°. Obtenir en fin de scrutin des résultats sécurisés et affichés en quelques minutes,
- 4°. Inscrire le processus électoral dans une démarche de préservation de l'environnement,
- 5°. Garantir la sécurité des opérations électorales et la confidentialité du vote.

IV. Modalités du scrutin électronique

Un scrutin est défini comme une opération de vote permettant d'élire les représentants d'un même collège électoral au sein d'une même instance.

L'ensemble des électeurs à un scrutin est rattaché à un seul bureau de vote. Lorsque plusieurs scrutins ont lieu en même temps, un bureau de vote centralisateur peut être créé.

En principe, le scrutin est de type liste à un tour, avec représentation proportionnelle au plus fort reste, sur des listes complètes et sans panachage. Des particularités peuvent cependant exister pour certains types de scrutin (ex. Commission consultative paritaire des agents non-titulaires, Conseil du Service de santé universitaire...), que le système de vote doit pouvoir prendre en charge.

Chaque identité électronique ne peut voter qu'une seule fois lors d'un même scrutin.

V. Acteurs des scrutins électroniques à l'Université

Les acteurs suivants sont impliqués dans toute opération de vote par voie électronique à l'Université :

- 1°. Le Président de l'Université décide de l'organisation du scrutin et en proclame les résultats ;
- 2°. Le Comité électoral consultatif de l'Université et éventuellement le Conseil d'administration, en cas de scrutin lié aux conseils centraux, émettent des avis sur le scrutin ;
- 3°. Un expert indépendant est chargé d'évaluer le système de vote (Lot n°2) ;
- 4°. Un prestataire est chargé de mettre à disposition le système de vote (Lot n°1) ;
- 5°. Une équipe, incluant du personnel de l'Université et du prestataire du système de vote, placée sous l'autorité du Directeur général des services de l'Université, est chargée de mettre en œuvre les opérations électorales et d'assurer les fonctions de centre d'appel et de cellule technique ;
- 6°. Des bureaux de vote électronique, et éventuellement un ou plusieurs bureaux de vote électronique centralisateurs ayant la responsabilité de plusieurs scrutins, veillent au bon respect des principes électoraux et à la bonne tenue des élections par voie électronique ;
- 7°. La Commission de contrôle des opérations électorales et, éventuellement, le Tribunal administratif compétent se chargent d'examiner les recours dirigés contre les scrutins.

VI. Qualité du prestataire mettant à disposition le système de vote et de l'expert mettant en œuvre l'expertise indépendant au regard de la loi informatique et libertés

En application de l'article 37 de la loi informatique et libertés, le prestataire qui exécute la mise en place du scrutin électronique et l'expert qui exécute la mise en œuvre de l'expertise indépendante sont qualifiés de sous-traitants. De ce fait ils ne peuvent agir que sur instruction de l'Université, qui est le responsable des traitements de données à caractère personnel intervenant lors des opérations électorales.

VII. Descriptions des prestations

Le présent cahier des charges définit et fixe les modalités de mise en œuvre du vote électronique et les engagements attendus de la part du prestataire du système de vote (Lot n°1), ainsi que de l'expert indépendant (Lot n°2).

A. Lot n°1 : le système de vote électronique

1. Prestations attendues

Le prestataire assure la conception, la gestion, la mise à disposition, l'hébergement et la maintenance d'un système de vote électronique à distance par internet, sécurisé et confidentiel. Est associés à cette prestation, la mise en place d'un système de secours en cas de panne du système principal.

Les prestations associées au système de vote incluent :

- 1°. La création et la personnalisation de la plateforme de vote par Internet (ex. respect de la charte graphique de l'Université, nom de l'Université dans l'adresse électronique...) ;
- 2°. L'animation de la présentation du système de vote au Comité électoral consultatif de l'Université, mentionnée au V.2° du présent document, avant le début des opérations électorales ;
- 3°. Des formations à l'utilisation du système de vote électronique pour les différents acteurs et participants du système de vote, notamment aux membres de l'équipe en charge des opérations électorales, aux membres des bureaux de vote et aux délégués de listes ;
- 4°. Les réunions de travail et l'accompagnement de l'équipe en charge des opérations électorales de l'Université, mentionnée au V.5° du présent document ;
- 5°. Les prestations liées à la transmission des informations nécessaires au vote, notamment la production d'un identifiant et d'un mot de passe strictement confidentiel pour chaque électeur et l'établissement et la répartition des clés de chiffrement pour chaque bureau de vote ;
- 6°. L'envoi du mot de passe strictement confidentiel, en vue de s'identifier sur la plateforme de vote, par mail et/ou par SMS ;
- 7°. La co-animation des cérémonies de scellement des urnes et de leur dépouillement, éventuellement à distance ;
- 8°. La relance, à travers le système de vote, par mail et/ou par SMS, des électeurs, au moment de l'ouverture du vote ;
- 9°. La relance, à travers le système de vote, par mail et/ou SMS, des électeurs n'ayant pas voté, lors du déroulement du scrutin ;
- 10°. Les garanties en termes de sécurité, intégrité et confidentialité du système pour toutes les étapes du scrutin, dont les tests préalables du système de vote électronique et du système de dépouillement tels que prévus à l'article 11-1 du décret n°2011-595 du 26 mai 2011 ;
- 11°. La participation au centre d'appel, à la cellule technique d'assistance et de maintenance, ainsi que l'assistance 24h/24h 7j/7j aux différents acteurs et électeurs dans la mise en œuvre du vote électronique pendant toute la durée du scrutin ;
- 12°. La documentation de présentation et les instructions techniques liées au système de vote ;
- 13°. Les prestations associées au dépouillement, à l'archivage et à la destruction des données ;
- 14°. L'aide à la publication des résultats en ligne ;
- 15°. La production de rapports d'incidents survenus ou neutralisés avant survenance pendant l'opération électorale ;
- 16°. Le suivi de la prestation à travers une enquête de satisfaction menée auprès des électeurs.

2. Les exigences légales s'appliquant aux prestations liées au système de vote

a. Le respect des principes fondamentaux encadrant les opérations électorales

La solution de vote électronique mise en œuvre par le prestataire respecte les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur auxquels sont soumises les opérations électorales, à savoir :

- 1°. L'accès au vote de tous les électeurs appelés à voter ;
- 2°. Le secret du scrutin ;
- 3°. Le caractère personnel, libre et anonyme du vote ;
- 4°. La sincérité des opérations électorales ;
- 5°. L'intégrité des suffrages exprimés ;
- 6°. La surveillance effective du vote durant son déroulement ;
- 7°. Le contrôle *a posteriori* par le juge de l'élection.

Le prestataire doit se conformer aux textes de références précités et en totale conformité avec les recommandations de la CNIL relatives au vote électronique.

Les garanties propres aux conditions de stricte neutralité, de confidentialité et d'hébergement des données, indiquées dans les textes cités dans le II du présent document, doivent être assurées dans tous les cas de figure et le prestataire choisi s'engage à les respecter, ainsi que l'ensemble des dispositions législatives et réglementaires en vigueur et régissant l'organisation de scrutin par voie électronique.

Le système mis à disposition pour l'Université doit faire l'objet d'une expertise préalable indépendante décrite dans le présent document, qui constitue le lot n° 2. Cette dernière est réalisée par un organisme indépendant, qui doit vérifier sa conformité à la législation en vigueur, en particulier au décret n°2011-595 du 26 mai 2011 susvisé. Le rapport de l'expert sur le système de vote sera transmis par l'Université à la CNIL et aux organisations syndicales présentant des candidats à un des scrutins. Le prestataire s'engage à déployer un système identique à celui certifié par l'expertise préalable.

Pour faciliter la validation de l'expertise, le prestataire doit fournir une matrice listant les recommandations de la CNIL et les réponses associées.

b. Livrables attendus du prestataire du système de vote

Le prestataire s'engage à déployer un système en conformité avec les textes régissant le scrutin et le présent document, identique à celui certifié par l'expertise préalable. Il s'engage à exécuter de bonne foi les prestations associées et nécessaires au bon déroulement du scrutin.

Avant toute opération électorale à travers le système de vote électronique et l'audit indépendant, le prestataire retenu doit fournir ou participer à la fourniture de :

- 1°. l'identification, la signature et le code source du logiciel mis à disposition pour l'opération de vote (à l'attention de l'expert indépendant) ;
- 2°. le rapport d'expertise comportant la signature du logiciel audité (en lien avec l'expert indépendant) ;
- 3°. la validation des préconisations de la CNIL (en lien avec l'expert indépendant) ;
- 4°. le matériel de vote mentionné au VIII.A.4 aux électeurs.

c. Sécurité et confidentialité

i. Obligation de confidentialité du prestataire

Le prestataire doit prendre connaissance, signer la clause de confidentialité fournie, et s'engage de ce fait à la respecter. Les obligations de discrétion, de confidentialité et de sécurité doivent s'imposer à l'ensemble des personnels du prestataire intervenant sur le système de vote électronique par internet.

Le prestataire s'engage à conserver de manière strictement confidentielle toutes les informations et les données qui lui seront transmises dans le cadre de l'organisation du vote électronique par l'Université.

ii. Niveau de sécurité du système de vote

Le système déployé doit comporter les mesures physiques et logiques permettant d'assurer la sécurité et la confidentialité des données transmises, à savoir : les fichiers utilisés pour établir les listes électorales, l'adressage des moyens d'authentification de l'électeur, de l'émargement, du scellement, de l'enregistrement et du dépouillement des votes. Il doit être conforme au référentiel général de sécurité prévu à l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005.

Le prestataire doit mettre en œuvre tous les moyens nécessaires pour sécuriser l'accès aux informations des fichiers fournis par l'Université. De plus il s'engage autant que nécessaire à limiter leur consultation aux seuls personnels habilités et autorisés pour l'exécution de la prestation.

Le niveau de sécurité et de confidentialité sera adapté en fonction de ou des l'arrêté(s) électoral(aux) pris pour le scrutin concerné. Le système de vote doit comprendre au moins deux niveaux de sécurité, dont :

- le niveau de sécurité 2 conformément aux recommandations de la CNIL n°2019-053 du 25 avril 2019 ;
- le niveau de sécurité 3 conformément à cette même recommandation.

Le prix de la prestation doit tenir compte du niveau de sécurité retenu par l'arrêté électoral ou les arrêtés électoraux pour chaque scrutin.

iii. Intégrité du système de vote

Le système déployé doit faire en sorte que chacun des scrutins puisse être isolé sur un système informatique indépendant, lorsque nécessaire.

Le système déployé doit assurer, pour chaque scrutin, des traitements informatiques distincts, dédiés et isolés, des données relatives aux électeurs sur les listes électorales ainsi que les données relatives aux votes, respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

Pendant la période de déroulement des scrutins, la liste d'émargement et l'urne électronique doivent faire l'objet d'un procédé garantissant qu'elles ne peuvent être modifiées respectivement que par l'ajout d'un émargement et l'ajout d'un bulletin, qui émanent d'un électeur authentifié et dont l'intégrité est assurée. Pendant cette même période :

- 1°. Les fichiers comportant les éléments d'authentification des électeurs et le contenu de l'urne doivent être inaccessibles ;
- 2°. La liste d'émargement et le compteur des votes ne doivent être accessibles qu'aux membres du/des bureau(x) de vote à des fins de contrôle de déroulement du scrutin ;
- 3°. Aucun résultat partiel ne peut être comptabilisé.

Le système de vote doit détecter les altérations de données. Les interventions sur le système de vote doivent pouvoir être réservées qu'aux seules personnes chargées de sa gestion et de sa maintenance et doivent pouvoir être détectées et retracées *a posteriori*.

iv. Transmission et destruction des données

Le prestataire s'engage à détruire les fichiers transmis et à ne conserver aucune de ces données, après l'exécution des opérations électorales et l'expiration des délais de recours.

Il s'engage aussi à transmettre à l'Université, en cas de défaillance du système de vote ou de litige, toutes les données utiles en sa possession.

d. Assistance juridique (prestation supplémentaire éventuelle (PSE 1))

Le prestataire et l'expert indépendant peuvent proposer (facultatif) une assistance juridique à l'Université en cas de contestation ou contentieux devant les juridictions compétentes.

Dans tous les cas, en cas de contentieux, le prestataire et l'expert indépendant s'engagent à fournir à l'Université toutes les informations utiles qu'ils auraient en leur possession concernant chaque opération électorale, objet du contentieux, sur laquelle ils ont eu à intervenir.

e. Analyse EBIOS (prestation supplémentaire éventuelle (PSE 2))

Le prestataire peut proposer (facultatif) une assistance pour mener l'évaluation des risques en informatique du système d'information de l'Université, en particulier l'analyse EBIOS.

f. Enquête de satisfaction (prestation supplémentaire éventuelle (PSE 3))

Le prestataire peut être appelé (facultatif) à opérer à travers le logiciel de vote, une enquête de satisfaction menée auprès des électeurs.

L'interface de cette enquête pourra être intégrée au logiciel de vote, afin d'être réalisée sous la forme d'un questionnaire soumis aux électeurs au terme de leur vote.

g. Adoption de délibérations par les instances lors de séances dématérialisées (prestation supplémentaire éventuelle (PSE 4))

Le prestataire peut proposer (facultatif) de déployer le logiciel de vote pour l'adoption de délibérations par les instances mentionnées dans le présent cahier des charges, pour assurer le respect du secret du vote, tel que mentionné à l'article 2 de l'ordonnance n° 2014-1329 du 6 novembre 2014 relative aux délibérations à distance des instances administratives à caractère collégial.

Ainsi, le logiciel remplit les exigences techniques pour garantir ce secret et doit ainsi permettre *a minima* :

- 1°. La saisie préalable des délibérations à voter,
- 2°. L'envoi des invitations à voter aux membres des instances concernées,
- 3°. Le suivi et la clôture des votes.

Cette prestation est exécutée en collaboration avec le président et les agents du service d'appui de l'instance concernée. Le service d'appui doit être capable de réaliser la saisie des points à l'ordre du jour soumis au secret du vote. Le président de l'instance doit pouvoir ouvrir et clôturer le vote sur ces points, d'en suivre le déroulement et de proclamer les résultats. Le vote doit pouvoir être recommencé en cas de problème. Le système utilisé doit pouvoir prévoir cette différenciation dans les droits.

h. Envoi d'une campagne de SMS en masse (prestation supplémentaire éventuelle (PSE 5))

Le prestataire peut proposer (facultatif) des campagnes de relances additionnelles relatives aux opérations électorales, notamment des campagnes de SMS en masse sur les numéros de téléphone portable saisis directement par les électeurs.

B. Lot n°2 : l'expertise indépendante

1. Prestations attendues

Un organisme, indépendant de l'Université et du prestataire, réalise une expertise indépendante, en amont et pendant le scrutin, qui doit être mise en œuvre afin de garantir que l'opération électorale répond aux exigences prévues dans les textes législatifs et réglementaires en vigueur, en particulier au décret n°2011-595 du 26 mai 2011 susvisé. Cet expert indépendant peut réaliser ses tâches d'expertise en présentiel ou à distance, en utilisant les outils appropriés et sécurisés pour les mener.

En principe, l'expertise doit comprendre :

- 1°. L'étude de la pertinence du niveau de risque estimé :
 - a. L'analyse du contexte du scrutin ;
 - b. L'analyse de l'étude menée par l'organisateur du scrutin ayant mené au choix du niveau ;
- 2°. L'étude du contexte spécifique de l'élection ;
 - a. L'analyse du protocole électoral, du décret éventuel ;
 - b. L'analyse de l'offre du prestataire de la solution de vote (optionnel) ;
- 3°. Le contrôle préalable au scrutin :
 - a. L'analyse des procédures mises en œuvre tout au long du projet ;
 - b. L'audit des infrastructures techniques d'hébergement de la solution de vote par internet ;
 - c. L'audit du code source de la solution de vote par internet ;
 - d. La participation à la génération des exécutables cibles et prise d'empreintes ;
 - e. La présentation de la démarche et de ses conclusions aux partenaires sociaux et autres acteurs ;
- 4°. Le contrôle pendant le scrutin :
 - a. La vérification de l'intégrité des exécutables ;
 - b. La vérification du respect des procédures ;
 - c. L'audit de la cérémonie de génération des clefs de l'élection et de scellement de la solution de vote par internet ;
 - d. Le suivi de la traçabilité pendant tout le scrutin ;
 - e. L'audit de la cérémonie de dépouillement et d'édition des résultats ;
 - f. La vérification de la mise sous scellés des éléments de contrôle *a posteriori* pour la durée de la période de recours contentieux ;

5°. Le contrôle après le scrutin :

- a. La participation aux contrôles a posteriori en cas de recours contentieux ;
- b. L'audit de la destruction des données conservées à l'issue de leur période de conservation.
- c. Tout contrôle/étude donne lieu à un rapport incluant au moins une synthèse, des conclusions et des recommandations.

2. L'indépendance de l'expert

L'expert doit se conformer à la délibération CNIL n° 2019-053 du 25 avril 2019 susvisée et par conséquent doit être un informaticien :

- 1°. Spécialisé dans la sécurité ;
- 2°. Indépendant de l'Université et du prestataire ;
- 3°. Possédant une expérience pertinente et suffisante dans l'analyse des systèmes de vote.

3. La démarche d'expertise

Préalablement à la mise en place ou à toute modification substantielle de sa conception, l'opération électorale à travers le système de vote électronique, l'expert retenu doit réaliser des contrôles et fournir à l'Université une expertise couvrant l'intégralité du dispositif installé avant le scrutin, les conditions d'utilisation du système de vote durant le scrutin, les conditions d'utilisation des postes dédiés au vote électronique ainsi que les étapes postérieures au vote.

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote décrits dans la délibération de la CNIL n°2019-053 du 25 avril 2019, et notamment sur :

- 1°. le code source correspondant à la version du logiciel effectivement mise en œuvre ;
- 2°. les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
- 3°. le système informatique sur lequel le vote va se dérouler ;
- 4°. les échanges réseau ;
- 5°. les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
- 6°. les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;
- 7°. l'évaluation du niveau de risque du scrutin ;
- 8°. la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

Lors de scrutins présentant un niveau de risque 2 ou 3, l'expert réalise des audits sur la plateforme de vote, afin de s'assurer de la cohérence et de l'effectivité des solutions apportées, par le biais de tests d'intrusions notamment. L'ensemble des opérations effectuées dans ce cadre est annexé au rapport d'expertise.

L'expert doit aussi fournir un moyen technique permettant de vérifier *a posteriori* que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise. Pour ce faire, l'expert peut, par exemple, utiliser des empreintes numériques.

4. Sécurité, intégrité et confidentialité

L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il est tenu de prendre toutes dispositions et précautions utiles 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.

L'expert doit prendre connaissance, signer la clause de confidentialité fournie, et s'engage de ce fait à la respecter. Les obligations de discrétion, de confidentialité et de sécurité décrites dans le présent document et dans la clause de confidentialité doivent s'imposer à l'ensemble des personnels de l'expert indépendant intervenant sur le système de vote électronique par internet.

5. Livrables attendus

Le rapport d'expertise, et ses annexes doivent être remis à l'Université et au prestataire de solution de vote par correspondance électronique via internet. Lié aux contrôles décrits, il doit comporter l'identification du logiciel audité et porter sur l'intégralité du code source utilisé par ce dernier.

Les rapports de l'expert sur le système de vote sont transmis par l'Université aux organisations syndicales présentant des candidats à un des scrutins et à la CNIL.

a. Etude du niveau de risque et du contexte électoral

En collaboration avec les acteurs impliqués dans l'opération de vote, l'expert indépendant contrôle la pertinence du niveau de risque estimé, en tenant compte du contexte de l'élection. Ces contrôles peuvent comprendre une analyse de l'offre du prestataire de la solution de vote.

L'étude qui en résulte est transmise au Président de l'Université et est annexée au rapport d'expertise synthétique préalable.

b. Rapport d'expertise synthétique préalable

i. Champ du rapport

L'expert indépendant doit fournir un rapport d'expertise synthétique préalable couvrant :

- 1°. l'intégralité du dispositif mis en place ;
- 2°. les conditions d'utilisation du système de vote durant le scrutin ;
- 3°. les conditions d'utilisation des postes informatiques mis à disposition des électeurs par l'établissement ;
- 4°. les étapes postérieures au vote. 12 CCTP

ii. Contenu et destination du rapport

Le rapport synthétique préalable de l'expert doit comporter, au moins :

- 1°. une grille de conformité à la recommandation de la CNIL ;
- 2°. une grille de conformité au RGS ;

- 3°. une analyse de la sécurité offerte par la solution et ses conditions de mise en œuvre selon les différents axes de sécurité (authentification, confidentialité, intégrité, traçabilité, procédures, conservation...) ;
- 4°. un rapport global sur les constats de l'expertise indépendante incluant ses conclusions.

Il est transmis au prestataire, ainsi qu'au Président de l'Université, qui le retransmet à la CNIL et aux délégués de liste des listes ayant déposé une candidature éligible au scrutin.

c. Rapport d'expertise détaillé

Outre le rapport d'expertise synthétique préalable et ses annexes, le rapport d'expertise final doit comprendre les contrôles réalisés pendant et après l'opération électorale, en incluant au moins :

- 1°. Le compte-rendu de l'audit des procédures, du code et de l'hébergement ;
- 2°. Le compte-rendu de la participation aux cérémonies ;
- 3°. Le compte-rendu de destruction.

Il comporte en annexe les résultats des analyses et tests réalisés par l'expert lors des divers contrôles réalisés en cours d'expertise.

d. Accompagnement en cas de recours (prestation supplémentaire éventuelle (PSE 1))

L'expert indépendant peut proposer (facultatif) un accompagnement juridique à l'Université en cas de contestation ou contentieux devant les juridictions compétentes.

Dans tous les cas, en cas de contentieux, l'expert s'engage à fournir à l'Université toutes les informations utiles qu'il aurait en sa possession concernant chaque opération électorale, objet du contentieux, sur laquelle il a eu à intervenir.

e. Observation des élections (prestation supplémentaire éventuelle (PSE 2))

L'expert indépendant peut proposer (facultatif) une prestation d'observation des élections.

VIII. Les modalités d'organisation du vote

A. Exigences préalables au déploiement du système de vote électronique

1. La séparation des données nominatives des électeurs et des votes

Le prestataire doit garantir l'anonymat du vote. De ce fait, le système déployé doit assurer que l'identité de l'électeur ne peut pas être associée avec l'expression de son vote. Cette séparation des données nominatives des électeurs et des votes doit être assurée à tout moment du processus de vote, y compris après le dépouillement.

2. Les sécurités informatiques

Le prestataire doit prendre toutes les mesures physiques (telles que le contrôle d'accès au système, la détermination précise des personnes habilitées à intervenir) et logiques (telle que la protection d'accès aux applicatifs et système utilisés) afin de garantir la sécurité et la confidentialité des données personnelles sur toute la durée et durant toutes les étapes du processus électoral. Cette obligation s'impose également pour le système de secours et d'assistance déployé.

Les algorithmes du prestataire doivent obligatoirement répondre aux exigences prévues dans le Référentiel Général de Sécurité (RGS).

Les algorithmes de chiffrement et de signature électronique doivent, dans tous les cas, être des algorithmes publics réputés « forts » et doivent, comme ces élections sont mises en place par une autorité administrative, impérativement répondre aux exigences prévues dans le Référentiel Général de Sécurité (RGS).

Pour assurer la conformité au RGPD, l'infrastructure du prestataire et de ses sous-traitants servant à l'hébergement des données relatives aux opérations électorales est obligatoirement située sur le territoire de l'Union européenne.

3. Le scellement du système de vote électronique

Avant le début du scrutin, le prestataire doit pouvoir vérifier que les modalités qui ont fait l'objet d'une expertise préalable par un organisme indépendant n'ont pas été modifiées. Il doit signaler toute modification opérée sur le système de vote depuis son évaluation par un expert indépendant, afin qu'il soit soumis à une nouvelle expertise.

Suite à cette vérification, le prestataire assure le scellement du système de vote électronique mis en place, la liste des candidats et des électeurs. Le scellement devra permettre de déceler toute modification du système déployé.

Le prestataire doit pouvoir assurer que la liste d'émargement des électeurs et l'urne électronique doivent faire l'objet d'un procédé garantissant qu'ils ne peuvent être modifiés que par l'ajout d'un bulletin de vote et de l'émargement, d'un électeur authentifié, pendant toute la durée du vote. Ce procédé retenu doit pouvoir déceler toute autre modification du système.

Après la clôture du vote, le prestataire assure le scellement de la liste d'émargement et l'urne électronique, avec des algorithmes respectant les recommandations du RGS.

Les scellements doivent pouvoir être vérifiés à tout moment de l'opération électorale.

Le prestataire doit permettre au bureau de vote de l'Université de disposer d'outils dont l'utilisation n'est pas soumise à l'intervention du prestataire, afin de procéder à la vérification de la régularité du scellement.

4. Identifiants et mots de passe

Le prestataire assure un système qui génère les identifiants et les mots de passe des électeurs.

Le système retenu doit assurer la transmission d'un mot de passe strictement individuel, généré aléatoirement et d'une complexité adaptée aux élections.

Afin d'assurer la sécurité de l'authentification, le prestataire proposera un système de lien web à usage unique permettant d'obtenir le mot de passe. Ce lien doit pouvoir être généré à nouveau, en cas de perte ou d'incident, sur demande de l'électeur après validation de la commission électorale.

Préalablement au scrutin, le prestataire enverra individuellement à chaque électeur, dans les délais prévus par le calendrier des élections, son identifiant, le lien unique pour générer son mot de passe, ainsi que l'adresse du site de vote électronique.

Le prestataire doit obligatoirement proposer deux modalités d'envoi de ces éléments :

- 1°. Soit par voie électronique : afin de garantir la confidentialité des moyens d'authentification, l'envoi doit se faire par au moins deux mails différents, transmettant respectivement, l'identifiant et l'accès au mot de passe ;
- 2°. Soit par voie postale : l'adresse de l'électeur sera fournie au prestataire avec la liste électorale.

Après avoir eu accès au site internet permettant de procéder aux démarches en vue de générer un mot de passe strictement confidentiel et individuel, ce dernier doit être envoyé soit par SMS, soit par mail.

5. La mise en place d'un dispositif de secours et d'assistance

Le système de vote électronique doit assurer la mise en place d'un dispositif de secours, en cas de panne ou de cyber attaque, du système principal. Celui-ci devra offrir à l'identique les mêmes garanties de sécurité et de confidentialité que le système principal. Le dispositif de secours doit pouvoir prendre immédiatement le relais en cas de défaillance du système principal, sans altération des résultats.

6. Le contrôle effectif du vote électronique

Le prestataire assure des mesures permettant de vérifier l'effectivité et l'efficacité des modules de sécurités mis en place pour assurer l'anonymat, la confidentialité et le secret du vote. Plus précisément le prestataire doit pouvoir assurer la vérification de :

- 1°. La garantie de confidentialité du fichier des électeurs comportant les éléments d'authentification ;
- 2°. Le chiffrement des bulletins de vote
- 3°. Le traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs

Le prestataire assure la conservation sécurisée des systèmes durant et après le déroulement des opérations électorales électroniques.

L'ensemble du système de vote électronique déployé (moyens informatiques centraux/ éventuellement déployé à l'Université même) doit être réalisé sous le contrôle et la surveillance effective, d'experts désignés par l'Université, et de représentants de l'Université.

Le prestataire doit accorder aux membres du/des bureau(x) de vote et aux délégués des candidats, s'ils le souhaitent, tous les moyens nécessaires pour assurer un contrôle effectif de l'ensemble du scrutin électronique. (En particulier de la préparation du scrutin, du vote, de l'émargement et du dépouillement.)

De ce fait, le prestataire assure une formation des acteurs de l'opération électorales au fonctionnement du système de vote électronique, et met à disposition de l'Université, des experts, et personnels, aux membres du/des bureau(x), des délégués des candidats, et scrutateurs. Il transmet également toutes notices et documents utiles à la compréhension et au fonctionnement du système déployé.

B. Le déroulement du scrutin électronique

1. L'accès à l'interface et le vote de l'électeur

Les membres du/des bureau(x) de vote ou du bureau de vote centralisateur et les personnes autorisées pour assurer la surveillance des opérations électorales, doivent pouvoir contrôler librement, les heures d'ouverture et de fermeture du scrutin électronique.

L'interface du système de vote doit permettre d'accéder à la documentation électeur détaillant le fonctionnement du système de vote, les détails sur le scrutin ou les scrutins (date d'ouverture, durée, clôture) et permettre une assistance, avant tout authentification.

Le système de vote retenu doit permettre à l'électeur de s'authentifier, à distance ou sur place/ au sein de l'Université, conformément au système préalablement décrit. Le système de vote ne doit pas permettre le vote de personnes ne figurant pas sur une liste électorale établie par l'Université par collège, propre à chaque instance, et transmise au prestataire, rectifiable au plus tard avant le scellement de l'urne électronique et l'ouverture du vote. Une fois l'urne électronique scellée, la liste électorale doit être figée et ne doit plus pouvoir être modifiée.

Le serveur de vote doit permettre la vérification de l'identité de l'électeur, et que son authentification est non-frauduleuse. L'authentification dans le système de vote peut être sécurisée par deux facteurs ou plus (ex. envoi d'un code SMS et/ou utilisation d'une information personnelle des électeurs). Suite à l'authentification, le système permet d'accéder aux listes électorales dans l'ordre officiel. Le vote blanc doit être prévu par le système électronique retenu. Si des électeurs sont communs entre deux scrutins ou plus, leurs identifiants et mots de passe demeurent les mêmes et le système de vote leur permet d'accéder par leur compte personnel aux scrutins pour lesquels ils sont électeurs et d'y exprimer leur voix qu'avec un seul compte.

L'électeur doit pouvoir accéder à l'information sur les candidatures (professions de foi, résolutions...), les bureaux de vote et les règles relatives au(x) scrutin(s) au(x)quel(s) il participe. Le système de vote doit donner la possibilité à l'électeur de pouvoir choisir une liste, un candidat ou un vote blanc. L'interface de vote doit pouvoir faire apparaître l'appartenance ou le soutien dont se prévalent les candidats. L'électeur accède aux listes de candidats ou aux sigles des organisations candidates, lesquels doivent apparaître simultanément à l'écran.

Le choix de l'électeur, lorsqu'il est réalisé, doit apparaître clairement à l'écran, indépendamment de toute autre information. Le système retenu doit donner la possibilité de revenir sur ce choix. La validation de son choix déclenche l'envoi du bulletin de vote dématérialisé vers le serveur des votes. Lorsque le vote est validé définitivement, l'électeur ne peut plus revenir sur son choix et ce choix est conservé dans l'urne de vote. La validation doit rendre le vote définitif et interdire toute modification ou suppression du suffrage exprimé. Le suffrage exprimé doit être anonyme et chiffré par le système et transmis dans un fichier « contenu de l'urne électronique » où il est conservé jusqu'au dépouillement. L'interface permet de visualiser le nombre de bulletins par urne et d'en suivre l'évolution en temps réel.

L'émargement doit faire l'objet d'un horodatage, tel que décrit au VIII.B.4 du présent document. La transmission du vote et l'émargement doivent faire l'objet d'un accusé de réception. La confirmation du vote doit être envoyée immédiatement à l'électeur, et il doit pouvoir conserver une trace de confirmation de son vote et l'imprimer, au besoin.

Le prestataire assure aux membres du/des bureau(x) de vote la possibilité de consulter l'évolution des opérations du scrutin électronique, pendant toute la durée du scrutin à travers la liste d'émargement et le nombre de votants.

2. La durée

Le système de vote doit permettre l'organisation d'un scrutin pouvant se dérouler pendant une période comprise entre vingt-quatre heures et huit jours. La durée de chaque scrutin est fixée par l'arrêté ou les arrêtés correspondant(s).

3. Le chiffrement du bulletin de vote

Dès son émission par l'électeur, le bulletin de vote doit être chiffré par un algorithme public réputé « fort » et stocké dans l'urne, sans avoir été déchiffré à aucun moment, même de manière transitoire.

La sécurité doit être assurée entre la liaison entre le terminal de vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement distinct de celui qui s'applique au bulletin pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote.

4. L'émargement

L'émargement électronique doit avoir lieu dès la validation du vote. L'émargement doit comporter un horodatage.

La liste d'émargement et le compteur des votes ne doivent être rendus accessibles qu'aux seuls membres du/des bureau(x) de vote habilités et toutes personnes autorisées par l'Université, uniquement à des fins de contrôle.

5. Le suivi des opérations électorales par les membres des bureaux de vote

Les membres du/des bureau(x) de vote disposent d'une interface de suivi propre, permettant de suivre la participation et le nombre de bulletins enregistrés dans l'urne en temps réel, consulter la liste des émargements, de surveiller le système de vote et d'en consulter les registres d'activité, de vérifier son intégrité et de répondre aux demandes des électeurs ne parvenant pas à se connecter, notamment concernant la rectification de données. Ils doivent pouvoir décider de l'interruption des opérations de vote, selon une procédure sécurisée nécessitant une double authentification, et déclencher la procédure de dépouillement en fin de vote à travers les clés de déchiffrement fournies.

6. Le dépouillement

Dès la clôture du scrutin, le contenu de l'urne, les listes d'émargement et les états courants gérés par les serveurs sont figés, horodatés et scellés automatiquement sur l'ensemble des serveurs, dans des conditions garantissant la conservation des données. Ainsi, avant le dépouillement, le système de vote doit garantir que l'urne et la liste d'émargement sont immédiatement scellés à la date de clôture du scrutin, afin de procéder au dépouillement. Le scellement du système doit pouvoir être contrôlé par le personnel habilité de l'Université et interdire toute reprise ou modification des résultats.

Toutes les informations nécessaires, et utiles à un contrôle *a posteriori*, doivent être recueillies durant cette étape. Elles doivent être stockées/enregistrées/scellées sur un support non réinscriptible.

Les clés de déchiffrement remises aux membres du/des bureau(x) préalablement désignés au moment de la création/génération des clés, doivent leur permettre d'actionner publiquement le dépouillement.

Les décomptes des votes doivent apparaître clairement à l'écran et faire l'objet d'une édition sécurisée, c'est-à-dire d'un mécanisme garantissant que l'affichage et l'impression des résultats correspondent au décompte de l'urne, pour être portés au procès-verbal de l'élection.

La procédure de décompte des votes enregistrés doit pouvoir être réalisée de nouveau, si nécessaire.

Le système de vote électronique doit être scellé 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 l'équipe électorale.

Une fois le dépouillement clôturé, les résultats proclamés peuvent être consultés à travers le système de vote et il est possible de consulter le procès-verbal, une fois celui-ci rendu public par l'Université.

7. Le suivi des opérations électorales par les membres de l'équipe électorale

Les membres de l'équipe électorale disposent d'une interface de suivi propre, permettant de suivre la participation en temps réel à l'ensemble des scrutins organisés, d'échanger en cas de besoin avec le prestataire en temps réel, de consulter les demandes de rectifications de données des électeurs et d'en proclamer les résultats une fois le dépouillement clôturé.

C. Le contrôle des opérations de vote électronique a posteriori

1. Les garanties minimales exigées pour un contrôle a posteriori

En cas de contentieux électoral, ou en cas de contrôle externe, le système de vote électronique retenu doit pouvoir être en mesure de fournir les éléments techniques permettant de prouver de manière irréfutable que :

- 1°. Le procédé de scellement n'a fait l'objet d'aucune intègre durant le scrutin ;
- 2°. Les clés de chiffrement et de déchiffrement n'ont été transmises et connues que de leurs seuls titulaires ;
- 3°. Le vote est anonyme et confidentiel ;
- 4°. La liste d'émargement ne comprend que la liste des électeurs ayant effectivement voté ;
- 5°. L'urne dépouillée a fait l'objet d'un traitement distinct et elle contient uniquement les votes des électeurs ;
- 6°. Le système retenu doit permettre à ce que la procédure de décompte des votes enregistrés puisse être déroulée de nouveau.

2. Enquête de satisfaction

Le prestataire peut être appelé à opérer un contrôle en lien avec le logiciel de vote, à travers une enquête de satisfaction menée auprès des électeurs.

Cette enquête pourra être intégrée au logiciel de vote et être réalisée sous la forme d'un questionnaire soumis aux électeurs au terme de leur vote.

Les résultats de l'enquête seront pris en compte pour le rapport final élaboré par la Présidente concernant l'opération électorale.

3. La conservation et l'archivage des données de l'opération électorales par voie électronique

Tous les fichiers supports (copies des programmes, matériels de vote, fichiers d'émargement, de résultats, sauvegardes, applicatifs) générés par le système de vote, doivent être conservés sous scellés pendant deux mandats et, en cas de litige, jusqu'à l'épuisement des voies et délais de recours, avant destruction sécurisée, ou versement aux Archives départementales pour les documents suivants :

- 1°. Les procès-verbaux des résultats, de proclamation de résultat et de dépouillement ;
- 2°. Un exemplaire du bulletin électronique de vote ;
- 3°. Les professions de foi.

Cette conservation doit être assurée, sous le contrôle de l'équipe en charge des opérations électorales mentionnée au V.5° du présent document, dans des conditions garantissant le secret et la confidentialité du vote. Cette conservation est assurée par le prestataire s'il est agréé par le service interministériel des Archives de France ou autrement par l'Université.

Si aucun contentieux électoral n'a été engagé avant la fin de l'épuisement des délais de recours, le prestataire s'engage à procéder à la destruction de l'ensemble des fichiers supports, après les avoir transmis dans leur intégralité aux services de l'Université, sous le contrôle du personnel de l'Université et des Archives départementales de la Vienne.

Des préposés du personnel du prestataire et des agents de l'Université participent à la destruction et/ou versement des données, qui se fait, dans tous les cas, sous le contrôle des Archives départementales de la Vienne.

D. Fichiers et traitements

1. Les fichiers fournis au prestataire par l'Université de Poitiers

Les listes électorales sont établies, contrôlées et transmises par l'Université de Poitiers à l'issue du travail des agents de l'équipe en charge des opérations électorales mentionnée au V.5° du présent document.

Le prestataire doit les intégrer à son système, qui doit offrir la possibilité d'accepter des éventuelles modifications jusqu'au premier jour du scrutin électronique.

Les listes de candidatures sont fournies par l'Université de Poitiers.

2. Traitement effectué sur les fichiers fournis

Le traitement et la transmission de ces fichiers au prestataire a pour finalité de :

- 1°. Délivrer à chaque électeur un moyen d'authentification ;
- 2°. Identifier les électeurs ayant pris part au vote ;
- 3°. Editer les listes d'émargement.

Ces traitements concourent au bon déroulement des opérations électorales.

Tout finalité à l'utilisation de ces fichiers non liée au bon déroulement des opérations électorales est prohibée.

Les listes doivent être enregistrées sur un support distinct de celui de l'urne électronique, scellé, non réinscriptible, rendant son contenu inaltérable et probant.

Le fichier correspondant au contenu de l'urne électronique recense uniquement les votes exprimés par voie électronique. Les données de ce fichier doivent être sécurisées et font l'objet d'un chiffrement. Ils ne doivent pas comporter d'éléments permettant l'identification des électeurs afin de garantir la confidentialité et le secret du vote.

Les données personnelles doivent être limitées au strict nécessaire afin de permettre le vote, et doivent être conformes à la loi Informatique et libertés ainsi qu'aux préconisations/recommandations de la CNIL.

IX. ASPECTS TECHNIQUES

A. Le déploiement et paramétrage du système de vote électronique

Le prestataire procède au déploiement et au paramétrage du système.

B. La phase préparatoire du vote électronique

La phase préparatoire a pour finalité de permettre au prestataire de préparer le système et d'intégrer les différentes listes électorales.

Durant cette phase, des tests programmés doivent alors lieu afin de contrôler le déroulement et la conformité du processus de vote durant une période préparatoire prévue dans le calendrier des élections.

Les tests interviendront après intégration des listes définitives (électeurs et candidatures) afin de fournir une simulation probante/ correspondante à la réalité. Les membres de l'équipe chargée de mettre en œuvre les opérations électorales, mentionnée au V.5° du présent document, seront requis comme votants afin de valider le bon fonctionnement du système.

C. Protocole de tests

Les tests du système auront lieu après le contrôle et la validation du processus d'élections, par l'expertise indépendante.

Les tests doivent être réalisés sur le système de vote électronique définitif et validés préalablement, afin de permettre aux membres du/des bureau(x) de vote de contrôler la conformité du système avant l'ouverture effective des élections.

Les étapes de contrôle doivent prévoir/ permettent le test de :

- 1°. La création par le bureau de vote, des clefs secrètes qui permettront le chiffrement des bulletins de vote dans le système et d'actionner le dépouillement ;
- 2°. L'ouverture des élections par le bureau de vote ;
- 3°. La réalisation de plusieurs votes selon des tests préparés par l'Université ;
- 4°. La clôture du scrutin par le bureau de vote ;
- 5°. Utilisation des clefs pour le déchiffrement des bulletins ;
- 6°. Dépouillement des urnes électroniques et la proclamation des résultats ;
- 7°. Contrôle de la conformité des résultats obtenus.

A l'issue du test, une validation du fonctionnement du système interviendra entre le bureau de vote, le comité d'organisation et le prestataire afin que le scellement puisse avoir lieu.

D. Livrable à l'Université

La fourniture des éléments permettant de tester l'intégralité des fonctions du système de vote une fois le paramétrage effectué, dont les clefs qui serviront au dépouillement à l'issue du scrutin de test.

X. CALENDRIER

Le prestataire devra fournir un calendrier prévisionnel comptable avec les contraintes calendaires suivantes :

Décision cadre portant sur l'organisation des élections par voie électronique	Avant l'organisation par l'établissement du premier scrutin par voie électronique
Expertise du système de vote + Transmission du rapport de l'expert à la CNIL et aux délégués des listes de candidats	Préalablement à la mise en place ou à toute modification substantielle de sa conception.
Prise de contact avec le rectorat	Lorsque le calendrier électoral est établi
Décision d'organisation de l'élection	Un (1) à deux (2) mois avant le début du scrutin
Prise de contact avec le Président de la CCOE	Lorsque le calendrier électoral est établi
Diffusion des informations nécessaires aux électeurs	Lorsque le calendrier électoral est établi
Établissement et contrôle des listes électorales	Lorsque le calendrier électoral est établi
Organisation matérielle du scrutin	Avant la date du scrutin
Affichage des listes électorales	Vingt (20) jours au moins avant le scrutin
Envoi d'une notice d'information aux électeurs	Au moins quinze (15) jours avant le premier jour du scrutin
Date limite demande d'inscription sur les listes électorales	Au plus tard cinq (5) jours francs avant la date du scellement de l'urne
Date limite de dépôt des candidatures	- Au moins quinze (15) jours avant le scrutin si envoi des candidatures et professions de foi aux électeurs par voie dématérialisée - Dans un délai compris entre quinze (15) jours francs maximum et cinq (5) jours francs minimum avant la date du scrutin si affichage des candidatures et professions de foi
Contrôle de l'éligibilité des candidats	Dans le délai prévu par la décision d'organisation des élections
Affichage des listes de candidats	A l'expiration du délai de rectification. Si envoi par voie dématérialisée des profession de foi et candidatures, l'affichage doit avoir lieu au moins quinze (15) jours avant le scrutin
Juste avant le scrutin	
Procéder aux test du système de vote	Avant le scellement de l'urne
Établissement et répartition des clefs de chiffrement + scellement du système de vote électronique	Avant le début du scrutin
Pendant le scrutin	
Contrôle du scellement du système	
Modification du système de vote	
Au terme du scrutin	
Scellement du système de vote électronique	Sur décision de clore le dépouillement prise par le président du bureau de vote
Proclamation et affichage des résultats	Dans les trois (3) jours suivant la fin des opérations électorales
Délai de recours devant la CCOE	Dans les cinq (5) jours à compter de la date d'affichage des résultats
Délai de recours devant le TA	Six (6) jours à compter de la date de notification de la décision du CCOE En l'absence de décision explicite, le tribunal administratif peut être saisi dans les six (6) jours suivant l'expiration d'un délai de deux mois à compter de la saisine de la CCOE
Conservation sous scellés des fichiers supports	Pendant un délai de deux (2) ans