Direction des systèmes d'information

MISE À DISPOSITION D'UN SYSTÈME DE VOTE ÉLECTRONIQUE ET ASSISTANCE À L'ORGANISATION, À LA PRÉPARATION ET AU DÉROULEMENT DES ÉLECTIONS DES INSTANCES DU CNRS

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n° 26373

Accord cadre n°26.14.019

Accord-cadre passé en application des articles L2125-1, R2124-1, L2124-2, R2124-2-1° et R2161-2 à 5 du Code de la Commande Publique, auquel il sera fait référence sous le vocable « le Code » dans la suite du présent document.

Objet : Ce document décrit les exigences fonctionnelles, techniques, d'intégration dans le SI, de sécurité et d'organisation des prestations pour la mise à disposition d'un système de vote électronique et assistance à l'organisation, à la préparation et au déroulement des élections du CNRS.

SOMMAIRE

MISE À DISPOSITION D'UN SYSTÈME DE VOTE ÉLECTRONIQUE ET ASSISTANCE À L'ORGANISATION, À LA PRÉPARATION ET AU DÉROULEMENT DES ÉLECTIONS DES INSTANCES DU CNRS 1

SOMMAIRE 2

TABLE DES ILLUSTRATIONS 3

1 CONTEXTE GÉNÉRAL 4

1.1 Contexte général des élections organisées par le CNRS 4
1.2 Objet de l'accord-cadre 4
1.3 Présentation synthétique du CNRS 6
1.4 Échéancier prévisionnel du projet 6
1.5 Lieu d'exécution de l'accord-cadre 6
1.6 Structure du CCTP et conventions de rédaction 7

2 CONTEXTE DU SI AU CNRS 8

2.1 Conformité réglementaire 8
2.1.1 Politique Générale de Sécurité des systèmes d'Information 8
2.1.2 Protection des données à caractère personnel (DCP) 9
2.1.3 Interopérabilité 12
2.1.4 Accessibilité numérique 12
2.2 Sites et utilisateurs du système d'information 14

3 DESCRIPTION DE LA SOLUTION 15

3.1 Objectifs de la solution 15
3.2 Exigences fonctionnelles 15
3.2.1 Exigences juridiques et de confidentialité 15
3.2.2 Acteurs (rôles) métier 16
3.2.3 Processus métier 17
3.2.4 Description fonctionnelle du service attendu 17
3.2.5 Fonctionnalités attendues du système ou cas d'utilisation 21
3.2.6 Communication des listes et professions de foi 25
3.3 Exigences de conduite du changement 26
3.3.1 Assistance à la conduite du changement 26
3.3.2 Foire aux questions et tutoriel 26
3.3.3 Assistance Utilisateur et organisateurs des élections 26
3.3.4 Formations 27

4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION 29

4.1 Exigences d'intégration dans le SI 29
4.2 Exigences techniques 29
4.2.1 Éléments techniques structurants 29
4.2.2 Engagements de qualité de service pour l'application 29
4.3 Exigences d'ergonomie-graphisme 30
4.3.1 Règles d'ergonomie 30
4.4 Exigences de sécurité 31
4.4.1 Auditabilité 32

5 CADRE D'ORGANISATION DES PRESTATIONS 33

5.1 Système qualité 33
5.2 Organisation des équipes projet 33
5.2.1 Organisation de l'équipe projet CNRS 33
5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire 34
5.3 Dispositifs de conduite de projet 34
5.3.1 Structures de pilotage projet 34
5.3.2 Pratiques de gestion de projet 34

5.3.3 Indicateurs de pilotage et qualité du projet....35
5.3.4 Activités de recette (à la charge du CNRS)....35
5.4 Gestion des environnements....35
5.4.1 Environnements....35
5.5 Gestion de la documentation....35
5.6 Mesures et clauses de sécurité....36
5.6.1 Gestion de la Sécurité par le titulaire....36
5.6.2 Protection des biens....48
5.6.3 Obligations du titulaire....51
5.6.4 Localisation des données....51
5.6.5 Audit....51
5.6.6 Application des plans gouvernementaux....52
6 ANNEXES....53
6.1 Présentation des directions du CNRS concernées....53
6.1.1 Le Secrétariat général du Comité national (SGCN)....53
6.1.2 La direction générale déléguée aux ressources (DGD-R)....53
6.2 Abréviations et Glossaire....55
6.2.1 Abréviations....55
6.3 Détail des scrutins par instances pour 2027....58
6.3.1 Élection pour le renouvellement des membres du CNESER....58
6.3.2 Election pour le renouvellement des représentants du personnel aux Conseils scientifiques d'institut....59
6.3.3 Election pour le renouvellement au Conseil scientifique....60

TABLE DES ILLUSTRATIONS

Figure 1 : Organisation du projet au CNRS.... 33

1 CONTEXTE GÉNÉRAL

1.1 CONTEXTE GÉNÉRAL DES ÉLECTIONS ORGANISÉES PAR LE CNRS

Le CNRS est doté de diverses instances consultatives nationales composées de membres élus et nommés.

Les élections organisées par le CNRS portent notamment sur :

- Le renouvellement des représentants du personnel au sein du conseil scientifique (CS) et des conseils scientifiques des instituts du CNRS (CSI),
- Le renouvellement des représentants du personnel au sein des commissions administratives paritaires (CAP), des commissions consultatives paritaires (CCP) et du comité social d'administration (CSA) du CNRS,
- Le renouvellement des représentants du personnel au sein du conseil national de l'enseignement supérieur et de la recherche (CNESER),
- Le renouvellement des représentants du personnel au sein du conseil d'administration (CA) du CNRS,
- Le renouvellement des représentants du personnel au sein des Sections du Comité national de la recherche scientifique,
- Le renouvellement des membres élus des commissions interdisciplinaires (CID) du Comité national de la recherche scientifique.

Dans une démarche de dématérialisation et de simplification préconisée au sein des établissements de l'État, le CNRS souhaite se doter d'un système de vote électronique (SVE) pour l'organisation et la tenue des prochaines élections.

Le principal enjeu tenant au déploiement et à l'utilisation d'un SVE pour ces scrutins est d'assurer la sécurité et l'attractivité de ce dispositif de vote.

Les objectifs poursuivis au travers de l'adoption du vote électronique sont la sécurisation, la modernisation et un accès large et facile du vote.

L'information et la communication auprès de l'ensemble des acteurs du vote électronique (administration, organisations syndicales et électeurs-trices) quant aux modalités de vote et à l'organisation de ces scrutins est également un objectif majeur.

Dans ce cadre, les exigences relatives au strict respect des cadres légaux et réglementaires, à la sécurisation des scrutins et à la maîtrise des délais constituent des enjeux majeurs de ce marché.

Il est prévu de conduire, au moyen de ce nouvel outil, les scrutins organisés par le CNRS, dès les scrutins programmés en 2027.

1.2 OBJET DE L'ACCORD-CADRE

L'accord-cadre a pour objet la mise à disposition d'un SVE et l'assistance à l'organisation, à la préparation et au déroulement des opérations électorales organisées par le CNRS.

Le SVE doit répondre de préférence aux objectifs de sécurité de niveau 3 tels que détaillés dans la délibération de la Commission nationale de l'informatique et des libertés n° 2026-045 du 19 mars 2026 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. À défaut, les objectifs de sécurité du niveau 2 doivent être satisfaits.

L'accord-cadre est passé par la Délégation Occitanie Ouest du CNRS, pour le compte de la direction des affaires juridiques (ci-après « DAJ ») du CNRS en tant que MOA et par la DSI du CNRS en tant que MOE.

Le présent CCTP décrit les prestations qui constituent le périmètre de l'accord-cadre ainsi que l'ensemble des règles et procédures à mettre en place pour garantir la bonne exécution des prestations par le titulaire et la fiabilité des opérations électorales sur le plan technique à toutes les étapes du traitement afin de sécuriser ces opérations et en garantir la régularité dans leur réalisation et suivi technique.

Les prestations attendues sont communes à toutes les élections qui seront organisées par le CNRS sur la durée de l'accord-cadre (y compris les reconductions éventuelles).

Pour l'année 2027, les scrutins suivants sont programmés (sous réserves) :

- le renouvellement des représentants du personnel au sein du Conseil national de l'enseignement supérieur de la recherche (CNESER),
- le renouvellement des représentants du personnel au sein du conseil scientifique (CS) et des conseils scientifiques des instituts du CNRS (CSI).

Les besoins en quantité sont susceptibles de varier en fonction des caractéristiques propres à chacune des élections (type de scrutin, nombre d'électeurs, nombre de collèges, nombre de candidats ou de listes de candidats, etc.), fixées par les textes réglementaires publiés avant le début de chaque campagne électorale, et qui seront communiquées par le CNRS au titulaire.

Au titre des prestations, il est attendu du titulaire :

- L'appropriation des besoins exprimés par le CNRS ainsi que le contexte de réalisation ;
- La mise à disposition du système de vote électronique à distance via internet dont l'accès se fait par le navigateur du votant, à partir de tout type de terminal (ordinateur, tablettes et smartphones) ;
- Des fonctionnalités d'administration ;
- Des prestations associées d'assistance et de conseil à l'organisation de ces élections décrites dans le présent CCTP et portant notamment sur :
    - Des prestations d'assistance à la rédaction des modalités électorales,
    - Des prestations d'assistance à la préparation du vote électronique,
    - Des prestations de conseil notamment sur les impacts fonctionnels, organisationnels et techniques pour la conduite du projet de déploiement et la mise en œuvre du vote électronique pour les élections ,
    - Des prestations de formation.

Au titre du SVE recherché, celui-ci implique une dématérialisation :

- Des listes électorales afin de constituer les listes d'émargement ;
- Des candidatures et des professions de foi et le cas échéant des CV ;
- Des urnes et du matériel de vote ;
- Du calcul et de la publication des résultats.

Le SVE doit respecter les principes généraux du droit électoral indispensables à la régularité du scrutin, à savoir :

- La sincérité et l'intégrité du vote : conformité entre le bulletin choisi par l'électeur et le bulletin enregistré dans l'urne électronique
- L'anonymat et le secret du vote : impossibilité de relier un vote émis à un électeur
- L'unicité du vote : impossibilité de voter plusieurs fois pour un même scrutin
- La confidentialité et la liberté du vote : exercer son droit de vote sans pression extérieure

Ces principes généraux devront être garantis par la sécurité des systèmes d'information et du SVE.

Le SVE doit s'adapter aux éventuelles évolutions réglementaires y compris en cas de réorganisation des élections.

Le SVE comprend les paramétrages mais aussi les développements informatiques réalisés spécifiquement pour couvrir les besoins du CNRS.

Au terme des articles R 211-505 à R211-527 du code général de la fonction publique relatifs aux 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'Etat, le SVE proposée permet d'assurer un strict respect des « principes fondamentaux qui commandent les opérations électorales : secret du vote, sincérité des opérations électorales, surveillance du scrutin et possibilité de contrôle par le juge ».

Elle doit être conforme aux dispositions réglementaires et aux recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL) applicables à cette élection. En conséquence, elle fera l'objet d'une inscription au registre de la Déléguée à la Protection des Données du CNRS préalable à l'élection.

Elle doit assurer un niveau permanent de sécurité conforme à l'état de l'art, ainsi qu'aux lois et réglementations applicables à ces élections.

Elle doit présenter une ergonomie claire, simple, intuitive afin de faciliter l'accès au vote par le plus grand nombre, y compris dans le cas d'électeurs malvoyants et non-voyants (conformité aux exigences du référentiel général d'accessibilité RGA V3.0 niveau AA).

1.3 PRÉSENTATION SYNTHÉTIQUE DU CNRS

Le Centre national de la recherche scientifique (ci-après : « CNRS ») est un organisme public de recherche (Etablissement public à caractère scientifique et technologique, placé sous la tutelle du Ministère de l'Enseignement supérieur, de la Recherche et de l'espace). Il produit du savoir et le met au service de la société.

Sa gouvernance est assurée par le président-directeur général du CNRS, assisté de directeurs généraux délégués.

Avec plus de 34 000 personnes, un budget de 4 milliards d'euros, une implantation sur l'ensemble du territoire national, le CNRS exerce son activité dans tous les champs de la connaissance, en s'appuyant sur plus de 1100 laboratoires.

Des chercheurs éminents ont travaillé, à un moment ou à un autre de leur carrière, dans des laboratoires du CNRS. Avec 21 lauréats du prix Nobel et 12 de la Médaille Fields, le CNRS a une longue tradition d'excellence.

- Présent dans tous les champs de la connaissance

Principal organisme de recherche à caractère pluridisciplinaire en France, le CNRS mène des recherches dans l'ensemble des domaines scientifiques, technologiques et sociétaux. Il couvre la totalité de la palette des champs scientifiques.

Le CNRS est présent dans toutes les disciplines majeures regroupées au sein de dix instituts (Institut des sciences biologiques, Institut de chimie, Institut écologie et environnement, Institut des sciences humaines et sociales, Institut des sciences de l'information et de leurs interactions, Institut des sciences de l'ingénierie et des systèmes, Institut national des sciences mathématiques et de leurs interactions, Institut de physique, Institut national de physique nucléaire et physique des particules et Institut national des sciences de l'univers).

Le CNRS développe, de façon privilégiée, des collaborations entre spécialistes de différentes disciplines, et tout particulièrement avec l'université, ouvrant ainsi de nouveaux champs d'investigations qui permettent de répondre aux besoins de l'économie et de la société. Des actions interdisciplinaires de recherche sont notamment menées dans les domaines suivants : « Le Vivant et ses enjeux sociaux », « Information, communication et connaissance », « Environnement, énergie et développement durable », « Nanosciences, nanotechnologies, matériaux » « Astroparticules : des particules à l'Univers ».

- Présent sur tout le territoire national et international

17 délégations en région assurent une gestion directe des laboratoires situés en métropole, en Outre-mer et à l'étranger.

Des informations plus complètes sont disponibles sur le site Web, à l'adresse suivante : http://www.cnrs.fr.

1.4 ÉCHÉANCIER PRÉVISIONNEL DU PROJET

Le projet démarre dès la notification de l'accord-cadre prévue fin décembre 2026.

Le titulaire propose dans son offre un planning visualisant les différentes phases du projet, prenant en compte les éléments précités.

Le planning est consolidé conjointement lors du démarrage de l'accord-cadre.

1.5 LIEU D'EXÉCUTION DE L'ACCORD-CADRE

Les comités, réunions ou ateliers de spécifications et de conception, nécessitant la présence du CNRS, se tiennent sur sites CNRS à Paris, ou en visioconférence entre ces sites.

Les modalités pratiques sont définies au démarrage de l'accord-cadre.

Les locaux du CNRS se situent :

à Paris (Siège du CNRS) :

CNRS - DAJ
3 rue Michel-Ange
75794 PARIS CEDEX 16

à Meudon (DSI) :

CNRS - DSI
1 place Aristide Briand
92195 MEUDON CEDEX

à Toulouse (DSI) :

CNRS - DSI
358 rue Pierre Gilles de Gennes
31670 LABEGE

1.6 STRUCTURE DU CCTP ET CONVENTIONS DE RÉDACTION

Le livret 1 du CCTP est composé essentiellement des chapitres suivants :

- contexte du SI au CNRS : contexte dans lequel s'inscrivent la réalisation et la maintenance de la solution, en terme de conformité réglementaire, d'infrastructure, d'urbanisation et d'intégration dans le système d'information existant,
- description de la solution : exigences métier et fonctionnelles pour la réalisation de la solution initiale,
- cadre de cohérence technique de la solution : exigences applicables à la solution initiale et à toute évolution lors de la maintenance de la solution,
- cadre d'organisation des prestations : exigences applicables aux processus de conduite de projet, développement et maintenance de la solution, ainsi que mesures de sécurité encadrant les prestations.

Le livret 2 du CCTP contient la description des prestations et unités d'œuvre, objets de la commande.

Les exigences vis-à-vis du titulaire sont décrites dans le présent document dans des tableaux de la forme ci-dessous. La référence est composée de 3 lettres définissant le groupe d'exigences (cf. « Référence des exigences » en annexe) et de 3 chiffres (pas nécessairement consécutifs). Les exigences sont classées selon 3 niveaux :

- Priorité 0 : exigence impérative à satisfaire obligatoirement par le titulaire
- Priorité 1 : exigence très fortement souhaitée, à justifier si non satisfaite
- Priorité 2 : exigence souhaitée, pouvant être satisfaite, partiellement ou pas par le titulaire (avec justification)

Référence	Libellé exigence	Priorité
XXX_NNN	Libellé de l'exigence	0/1/2

2 CONTEXTE DU SI AU CNRS

2.1 CONFORMITÉ RÉGLEMENTAIRE

Les applications mises en œuvre par le CNRS sont soumises à des conformités réglementaires définies dans des référentiels interministériels présentés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
REGL_001	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels : Sécurité (RGS), Interopérabilité (RGI, selon le profil choisi par le CNRS) et Accessibilité (RGAA, niveau AA, avec certification externe). RGS : https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/referentiel-general-de-securite/ RGI : https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/rgaa RGAA : https://accessibilite.numerique.gouv.fr/ (https://a11yproject.com)	0
REGL_003	La page d'accueil de la solution permet d'accéder aux mentions légales : licence d'utilisation du logiciel, point de contact éditorial et technique, éventuelles mentions légales réglementaires concernant les données à caractère personnel, l'utilisation des cookies.	0

2.1.1 Politique Générale de Sécurité des systèmes d'Information

Concernant les aspects sécurité, les objectifs de la Politique Générale de Sécurité des systèmes d'Information (PGSI[1]) du CNRS sont les suivants :

- Protéger le savoir-faire du CNRS et les données permettant de valoriser la recherche ;
- Assurer la protection du potentiel scientifique et technique et le respect des engagements internationaux ;
- Garantir la disponibilité des moyens opérationnels du CNRS ;
- Assurer le respect par le CNRS de ses obligations légales, réglementaires et contractuelles ;
- Éviter les accidents qui résulteraient de la perte de contrôle d'un processus ou tout au moins en limiter les conséquences ;
- Conserver au CNRS un statut de partenaire de confiance.

A ces fins, le CNRS applique les principes de politique générale suivants (issus de la PGSI du CNRS) :

- L'ensemble du périmètre placé sous la responsabilité du CNRS doit être couvert ;
- Toutes les exigences légales et réglementaires doivent être prises en compte ;
- La gestion des risques doit être réalisée de façon systématique suivant la réglementation Française et les normes internationales en vigueur ;
- L'organisation qui est mise en place pour piloter et mettre en œuvre cette politique doit disposer des moyens humains compétents en nombre suffisant ;
- Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
- L'application de cette politique est contrôlée.

D'un point de vue contractuel, le titulaire doit respecter au minimum les exigences sécurité du présent CCTP.

[1] **PGSI :** document diffusable sur demande à l'équipe sécurité de la DSI du CNRS

Référence	Libellé exigence	Priorité
REGL_004	Le titulaire se conforme au cadre réglementaire applicable en termes de SSI, à savoir (de façon non exhaustive) : ▪ les annexes techniques du Référentiel Général de Sécurité (RGS) ▪ la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E) ▪ l'instruction interministérielle 901 (II901) portant sur les informations sensibles marquées « diffusion restreinte » ▪ la PSSI du CNRS (PSSI-C) RGS : https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/referentiel-general-de-securite/ PSSI-E : https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-du-service-numerique-de-letat/ II901 : https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-information-sensible-diffusion-restreinte/instruction-interministerielle-n901/ PSSI-C : Document non public, disponible sur demande	0
REGL_005	D'un point de vue technique, le titulaire applique les différents guides de l'ANSSI : https://cyber.gouv.fr/offre-de-service/guides-services-numeriques-et-outils/	1

2.1.2 Protection des données à caractère personnel (DCP)

Dans le cadre de réalisation de la prestation, des traitements de données à caractère personnel sont réalisés.

Les traitements effectués doivent être conformes au règlement n°2016/679 du 27 avril 2016 relatif la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), à la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et aux textes pris pour son application.

Le processus global et chacun des éléments constitutifs du SVE sont **impérativement** conformes :

- à la délibération de la CNIL n° 2026-045 du 19 mars 2026 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. ;
- aux analyses et recommandations de la CNIL.

Le CNRS est responsable des traitements dont la finalité porte sur l'organisation des élections des représentants au sein des diverses instances du CNRS.

Le titulaire du marché est sous-traitant au sens de la règlementation sur la protection des données pour cette finalité. Il est chargé de fournir la solution de vote électronique et d'assister le CNRS dans les différentes phases des opérations électorales.

Les données personnelles sont traitées aux seules fins des prestations décrites dans l'accord-cadre et ses marchés subséquents, conformément à l'article 28 du RGPD et à l'article 60 de la loi Informatique et libertés.

Les types de données personnelles concernées sont notamment :

- Des données d'identification : nom, prénom, date de naissance ;
- Des données relatives à la vie professionnelle : Unité d'affectation - Catégorie (chercheur ou ITA) - Dates de début et de fin de contrat - Corps - Grade- Institut Adresse professionnelle CV, profession de foi, matricule Sirhus ;
- Des données de connexion : logs de connexion au site de vote ;
- D'autres données : Identifiants électoraux, donnée secrète pour le vote électronique.

Les données sont pour partie hautement sensibles et impliquent la réalisation d'analyses d'impact sur la vie privée par les responsables de traitement. Le titulaire s'engage à apporter son concours à ces analyses.

Les personnes concernées sont les agents CNRS ou non, travaillant dans une unité rattachée au CNRS.

Les obligations des parties

Chaque Partie s'engage à respecter l'ensemble des exigences liées à la protection des données personnelles conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du règlement européen n°2016/679 sur la protection des données personnelles.

Les Parties assurent et préservent la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement et des données personnelles et documents contenus dans le périmètre relevant de leurs attributions.

Le CNRS en tant que responsable de traitement inscrit le traitement de données personnelles dans le registre des traitements de données tenu par la Déléguée à la Protection des Données du CNRS.

Conformément aux dispositions de l'article 28 du RGPD et de l'article 60 de la loi Informatique et libertés, le sous-traitant s'engage à :

- traiter les données uniquement dans le cadre de la prestation ;
- traiter les données conformément aux dispositions de la prestation et à toute autre instruction du responsable du traitement. Dans l'hypothèse où le sous-traitant estimerait qu'une instruction documentée du responsable du traitement dans le cadre de la prestation pourrait être considérée comme illicite au regard du RGPD ou de la loi Informatique et libertés, il s'engage à en informer immédiatement le responsable du traitement, étant précisé que celui-ci sera seul juge de la validité des instructions données et que cette information ne saurait en aucun cas suspendre la bonne exécution de la prestation par le sous-traitant.

Le titulaire tient un registre des traitements des données qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).

Les Parties se communiquent le nom et les coordonnées de leur délégué à la protection des données respectivement désigné.

Les Parties s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information ou de contrôle.

Chaque Partie demeure responsable des dommages qui lui seraient imputables concernant la protection des Données à caractère personnel faisant l'objet d'un traitement dans le cadre de l'exécution des Prestations (ex : fuite ou perte de données, intrusion informatique, etc.).

Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

Il met à la disposition du CNRS toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le CNRS ou tout auditeur dûment mandaté par lui.

Recours à des sous-traitants

Le titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. Le CNRS demande communication de ces engagements lors de la phase de consultation et est à tout moment autorisé à vérifier, conformément à la clause d'audit, la réalité de cet engagement.

Le titulaire s'engage à notifier et obtenir l'accord expresse de l'Acheteur de toute modification ou recours à un sous-traitant/hébergeur. En toute hypothèse, le traitement des données par le sous-traitant ou par l'hébergeur doit respecter les dispositions applicables en matière de protection des données personnelles.

Il appartient au titulaire de s'assurer qu'ils présentent les mêmes garanties quant à la mise en œuvre des mesures techniques et organisationnelles appropriées ainsi que les mesures de sécurité, de manière à ce que le traitement réponde aux exigences des dispositions en vigueur.

Confidentialité

Les données transmises, collectées, exploitées par le titulaire sont, pour partie des données à caractère personnel dont la sensibilité est forte au sens de la règlementation sur la protection des données personnelles.

Le titulaire veille à ce que les personnels autorisés à traiter les données à caractère personnel s'engagent à en respecter la confidentialité ou soient soumis à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

L'information et le droit des personnes

Il est convenu que le CNRS est seul tenu de l'obligation de fournir aux personnes dont les données sont traitées l'ensemble des informations requises par les articles 13 et 14 du RGPD.

Par ailleurs, il est tenu du traitement des demandes des personnes concernées par ces traitements dans le cadre de l'exercice de leurs droits conformément aux articles 15 et suivants du RGPD.

Le titulaire s'engage à apporter son aide et communique toute information dont le CNRS aurait besoin pour s'acquitter de ces obligations.

La sécurité des données

Le titulaire s'oblige à prendre toutes précautions utiles afin de les protéger contre toute destruction accidentelle ou illicite, perte, altération, diffusion et de garantir que les données ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

Il met à la disposition du CNRS toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le CNRS ou tout auditeur dûment mandaté par lui.

Les mesures respectent les exigences décrites à l'article 5.6 du présent CCTP.

Durées de conservation des données, archivage, destruction

Les données sont traitées selon les dispositions décrites au 3.2.5.5.

Traitement des incidents impactant les données à caractère personnel

Le titulaire s'engage à communiquer au CNRS dans les meilleurs délais, et sous 48 heures au plus tard après en avoir pris connaissance, la survenance de toute faille de sécurité ayant des conséquences directes sur le traitement des données personnelles ou sur le fonctionnement du système de traitement. Il lui fournit notamment toute information relative à la nature de la violation, au nombre de personnes concernées, aux catégories et au nombre d'enregistrements de données à caractère personnel concernés, ainsi qu'aux conséquences probables de la violation, aux mesures prises pour y remédier et atténuer les éventuelles conséquences négatives. Il conserve en outre tout document relatif à la violation de données, ses effets et les mesures prises pour y remédier.

Le titulaire intervient dans le processus de gestion des incidents de sécurité liés à l'application ; son aide est requise pour :

- Évaluer l'impact d'un incident de sécurité sur les DCP (*par exemple* : divulgation de données, modification non autorisée des données, suppression de données…) en nombre d'utilisateurs et en quantité de données exposées ;
- Fournir les correctifs nécessaires à la résolution de l'incident.

Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la réglementation.

Le niveau de priorité accordé aux incidents de sécurité impactant les DCP est automatiquement le niveau le plus élevé.

Audit

Le responsable du traitement dispose du droit de faire procéder à ses frais, par ses services ou tout tiers de son choix, à un audit du sous-traitant en vue de vérifier le respect par ce dernier de ses obligations au titre de la présente annexe.

L'audit devra être effectué de manière à préserver les informations confidentielles détenues par les PARTIES et à garantir le respect du secret professionnel.

Le sous-traitant s'engage à permettre et à faciliter la réalisation de ces audits, notamment par la mise à disposition du personnel et de toute la documentation nécessaire et utile à la bonne mise en œuvre des opérations d'audit.

L'audit pourra avoir lieu maximum une fois pendant toute la durée du CONTRAT et à tout moment (i) en cas de suspicion de violation du RGPD ou de la loi Informatique ou libertés ou (ii) pour faire vérifier la mise en place des actions correctives demandées par l'autre PARTIE.

L'audit ne pourra être mis en œuvre qu'à des horaires d'ouverture des bureaux normaux et sous réserve d'un préavis de 10 jours ouvrés, adressé par écrit au sous-traitant et comprenant la désignation des personnes ou entités missionnées par le responsable du traitement pour y procéder. La présence de l'auditeur dans les locaux du sous-traitant ne pourra pas excéder un jour.

Le responsable du traitement s'engage à ce que l'auditeur présente des garanties de confidentialité suffisantes au regard de la nature des informations auxquelles il pourrait accéder dans le cadre de l'audit.

Le sous-traitant pourra s'opposer à la désignation d'un auditeur tiers spécifique si, pour des raisons objectives tenant à sa situation, la réalisation de l'audit par cet auditeur tiers pourrait manifestement lui causer un préjudice direct.

En aucun cas, l'exercice de la faculté de s'opposer à cet audit ne saurait avoir pour objet ou pour effet d'empêcher toute réalisation de l'audit visé par le présent article.

Une copie du rapport d'audit sera remise à chaque PARTIE. Toute recommandation formulée dans le cadre de l'audit sera examinée et les points critiques seront corrigés.

Dans le cas où le rapport d'audit ferait apparaître une irrégularité, la PARTIE concernée s'engage, dans le cadre d'un plan d'action, à mettre en œuvre à ses frais les mesures correctives nécessaires pour y remédier dans un délai raisonnable à compter de la remise du rapport.

2.1.3 Interopérabilité

Le référentiel général d'interopérabilité (RGI) est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.

Le RGI est défini dans 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. Dans l'article 11 de cette ordonnance, le « RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret ».

Le référentiel général d'interopérabilité applicable est disponible en libre accès :

https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/

Le titulaire respecte les dispositions du profil d'interopérabilité P1 choisi par le CNRS conformément aux objectifs du présent accord cadre. Le profil P2 sera également utilisé comme référence en cas d'utilisation de webservices.

2.1.4 Accessibilité numérique

2.1.4.1 *Contexte*

Comme le définit l'article 47 de la loi 2005-102 du 11 février 2005, est concerné par l'obligation légale d'accessibilité tout type d'information sous forme numérique quels que soient le moyen d'accès, les contenus et le mode de consultation.

Plus précisément, sont concernés tous les documents ou applications disponibles depuis un navigateur web : les sites Internet et Intranet (ces derniers étant des outils de travail courants pour les salariés handicapés, lesquels doivent pouvoir accéder à toutes les informations nécessaires à l'exécution de leurs missions), et les applications web.

Par application web, on entend toute application « métier » à laquelle on accède au moyen d'un navigateur web et qui vise tout ou partie des agents d'un ministère, d'un organisme public ou le grand public.

2.1.4.2 *Niveau attendu pour l'accessibilité numérique*

La solution doit prendre en compte le niveau légalement attendu pour l'accessibilité numérique qui est à ce jour le niveau double A (AA).

Le référentiel d'accessibilité applicable est disponible en libre accès :

https://accessibilite.numerique.gouv.fr/

et plus précisément le référentiel technique d'accessibilité :

https://accessibilite.numerique.gouv.fr/ressources/

Les critères à retenir du référentiel général d'accessibilité pour les administrations (RGAA) dans sa version 3.0 sont donc tous ceux permettant de répondre aux niveaux déduits [A] et [AA] du WCAG (Web Content Accessibility Guidelines).

Niveaux de conformité WCAG :

Niveau	Définition de la conformité	Critères
A (niveau minimal)	La page web satisfait à tous les critères de succès de niveau A ou une version de remplacement est fournie.	Critères de succès essentiels pouvant raisonnablement s'appliquer à toutes les ressources web.
AA	La page web remplit tous les critères de succès de niveau A et AA ou une version de remplacement conforme au niveau AA est fournie.	Critères de succès pouvant raisonnablement s'appliquer à toutes les ressources web.

2.1.4.3 *Certificat de conformité*

Référence	Libellé exigence	Priorité
REGL_006	Pour les téléservices destinés aux usagers, le titulaire fait son affaire de la fourniture à la livraison de la solution d'un certificat de conformité à la réglementation sur l'accessibilité numérique des contenus web, certificat établi par un organisme certificateur européen reconnu et compétent mentionnant une conformité d'au moins 80%. Elle prévoit la mise en ligne sur le site ou l'application de la déclaration de conformité et des dérogations déclarées et justifiées.	0
REGL_007	Pour les solutions qui ne sont pas des téléservices, le titulaire prévoit la mise en ligne sur le site ou l'application des mentions de conformité et dérogations à la réglementation sur l'accessibilité numérique fournies par le CNRS en indiquant le niveau de conformité constaté.	1

La déclaration de conformité établie sur la base du certificat de conformité porte **au minimum** sur la liste des pages suivantes du site ou de l'application, lorsqu'elles existent :

- *Page d'accueil* (page constituant le point d'entrée principale du service, elle est généralement accessible par une adresse de la forme http://www.urldusite.extension ; pour le CNRS en particulier, cette adresse a la forme suivante : https://appli.cnrs.fr) ;
- *Page contact* (page contenant les informations de contact ou le ou les formulaires permettant de contacter directement le ou les responsables du service) ;
- *Page mentions légales* ;
- *Page politique d'accessibilité* : outre les informations relatives à l'évolution globale de l'accessibilité du site ou de l'application, cette page contient les renseignements relatifs à la déclaration de conformité dont la liste des pages ou secteurs du service dérogeant aux exigences d'accessibilité, leur type de contenu et les solutions alternatives pour y accéder ;
- *Page aide* (page contenant les informations facilitant l'utilisation du site ou de l'application, raccourcis claviers, éventuels, logiciels/plug-in nécessaires à la consultation). La page d'aide, obligatoire, doit mentionner les coordonnées d'un contact au sein de l'administration et les coordonnées du défenseur des droits (http://www.defenseurdesdroits.fr/) ;
- *Page plan du site* (page récapitulant l'arborescence du site ou permettant plus largement une navigation au sein des différentes pages composant le service) ;
- *Page recherche* (page dont l'objet principal est la mise à disposition d'un formulaire de recherche ou des résultats d'une recherche) ;

- *Toutes les pages composant le processus* principal de l'application ou du service en ligne (un formulaire ou une transaction sur plusieurs pages).

2.2 SITES ET UTILISATEURS DU SYSTÈME D'INFORMATION

Les utilisateurs du système d'information du CNRS sont principalement répartis :

- dans les 18 délégations, en régions et en Ile de France et sur le siège parisien de l'établissement. Ils représentent environ 3000 agents, dotés principalement de poste de travail de type PC sous Windows ;
- dans l'ensemble des laboratoires, répartis sur l'ensemble du territoire. Ils représentent plus de 60 000 personnes potentiellement utilisateurs du système d'information dont plus de 30 000 agents CNRS.

3 DESCRIPTION DE LA SOLUTION

3.1 OBJECTIFS DE LA SOLUTION

Les prestations, objets de ce marché, portent sur le vote électronique à l'exclusion de toute autre modalité de vote qui pourrait lui être associée.

3.2 EXIGENCES FONCTIONNELLES

3.2.1 Exigences juridiques et de confidentialité

La mise en œuvre du système de vote électronique (SVE) doit être conforme aux exigences posées par le cadre légal et réglementaire en vigueur au moment du scrutin, notamment :

Textes applicables
Articles R 211-505 à R 211-527 du code général de la fonction publique relatifs aux 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.
Guide **ANSSI** de « Recommandation pour la mise en œuvre du vote par Internet pour les élections non politiques »
Délibération de la CNIL **n° 2026-045 du 19 mars 2026** portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
Décret n° 2010-112 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.
Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité (RGS) et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD).
Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Exigences juridiques

Référence	Libellé exigence	Priorité
EJ_001	Le SVE proposé est conforme aux textes listés au § 3.2.1	0
EJ_002	En particulier, le SVE est impérativement conforme à la recommandation de la CNIL adoptée le 19 mars 2026 relative à la sécurité des systèmes de vote par correspondance électronique. Le vote électronique respecte notamment : ▪ Les principes démocratiques indispensables à la régularité du scrutin, à savoir la possibilité effective pour chaque électeur d'exprimer son vote, y compris par un vote blanc ; ▪ Le secret du bulletin, le vote libre et confidentiel ; il doit s'exercer sans pression extérieure ; ▪ Le caractère personnel et anonyme du vote : impossibilité de relier l'expression d'un vote émis à un électeur ; ▪ La sincérité des opérations électorales : intégrité du vote en respectant le vote choisi par l'électeur ; ▪ L'unicité du vote : impossibilité de voter plusieurs fois pour un même scrutin ; ▪ La sécurité des opérations et la surveillance effective du scrutin : confidentialité des données des fichiers constitués pour établir les listes électorales, sécurisation de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et le dépouillement des votes ; ▪ Le contrôle a posteriori par le juge en cas de recours contentieux.	0

Référence	Libellé exigence	Priorité
EJ_003	Le SVE répond de préférence aux objectifs de sécurité de niveau 3 tels que détaillés dans la délibération de la CNIL n° 2026-045 du 19 mars 2026	1
EJ_004	Le SVE répond aux objectifs de sécurité de niveau 2 tels que détaillés dans la délibération de la CNIL n° 2026-045 du 19 mars 2026 Par dérogation, la solution doit impérativement respecter les objectifs définis dans la délibération CNIL n° 2019-053 dès la notification du marché. **Pour les objectifs définis dans la délibération CNIL n°2026-045 qui ne seraient pas atteints à cette date, le titulaire fournit, à l'appui de son offre, la roadmap d'évolutions de sa solution qui garantit l'atteinte de ces derniers au plus tard 12 mois après la notification du marché.**	0

Exigences de Confidentialité

Référence	Libellé exigence	Priorité
CONF_001	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 équipes électorales recueillies aux fins de création de leurs comptes sur le SVE, ne peuvent être utilisés qu'aux fins du vote décrites dans le présent document et ne peuvent être divulgués sous peine de sanctions prévues par le code pénal. Le titulaire se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées par le CNRS.	0
CONF_002	Le SVE fournit et assure la confidentialité des données transmises, à savoir : Les listes des électeurs par scrutin (pseudonymisées), Les listes d'émargement, Le dépouillement des votes.	0
CONF_003	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 listes des opérations effectuées sur la plate-forme, etc.) gérées par le SVE et/ou conservées à l'issue du vote, sont la propriété du CNRS et doivent faire l'objet d'un traitement garantissant leur confidentialité.	0
CONF_004	La confidentialité des données électorales est également opposable aux administrateurs techniques en charge de la gestion ou de la maintenance du système informatique.	0
CONF_005	Le titulaire s'engage à respecter une clause de confidentialité et de sécurité et à la faire respecter par son personnel. Il fournit au CNRS le descriptif détaillé du dispositif technique mis en œuvre pour assurer cette confidentialité. Il se porte garant et fait en sorte que l'ensemble de ses sous-traitants s'engagent dans les mêmes conditions de confidentialité et de sécurité.	0
CONF_006	Le système de vote du titulaire permet de s'assurer de l'identification et de l'authentification de l'électeur. Il doit garantir la confidentialité des moyens fournis à l'électeur pour l'accès au vote et prendre toutes précautions utiles afin d'éviter qu'une personne non autorisée se substitue frauduleusement à l'électeur.	0

3.2.2 Acteurs (rôles) métier

Électeurs : Agents CNRS ou personnels de l'ESR (Enseignement supérieur et de la recherche) remplissant les conditions réglementaires pour prendre au vote en fonction des instances concernées.

Organisations syndicales : Organisations syndicales représentatives pouvant faire acte de candidature lors des différents scrutins.

Candidats : Personnels ESR ou Organisations syndicales pouvant déposer une candidature lors du renouvellement des membres élus d'une instance.

Bureau de vote électronique et membres du bureau de vote électronique (BVE) : Chaque scrutin propre à une instance de représentation des personnels donne lieu à la constitution d'un bureau de vote électronique composé d'un président, un secrétaire et les délégués des listes candidates.

Cellule d'assistance technique : Cellule composée de représentants du CNRS et de préposés du prestataire. La cellule mise en place par le CNRS est chargée de veiller au bon fonctionnement et à la surveillance du SVE.

Le pôle Conseil d'administration ressources élections (CARE) de la direction des affaires juridiques du CNRS, ci-après désigné « CARE-CNRS », est chargé de l'organisation et de la réalisation des élections de ces instances, organisées par le CNRS.

3.2.3 Processus métier

La mise en place et l'organisation d'un scrutin de vote électronique se décomposent en plusieurs étapes comme décrites dans le tableau ci-après.

Processus	Action	Détail
Pré-électoral	Présentation du SVE aux organisations syndicales	Organiser des réunions d'information avec les organisations syndicales tout au long du processus
	Constitution, intégration dans le SVE et publicité des listes électorales	Intégrer les listes électorales dans le SVE et publier les listes électorales
	Gestion et publicité des candidatures, logos et professions de foi	Intégrer et publier les candidatures, les sigles et les professions de foi
		Remplacer un candidat
	Déploiement des moyens de vote à destination des électeurs	Envoi des identifiants et des notices de vote
		Réassorts éventuels
	Déploiement des moyens de vote à l'usage des BVE	Former les membres des BVE
		Mettre en place les BVE
		Tester au préalable le dispositif de vote électronique global
		Générer et remettre les clés de chiffrement
		Tester le dispositif au niveau de chaque scrutin
		Effectuer le scellement
Electoral	Vote	Ouvrir le scrutin
		Voter (électeur)
		Superviser le vote
		Suspendre le scrutin
		Reprendre le scrutin
		Clôturer le scrutin et sceller le SVE
	Dépouillement	Décompter les voix obtenues par chaque candidature
		Inscrire sur le procès-verbal le décompte des voix obtenues par chaque candidature et la répartition des sièges
		Clôturer le dépouillement et effectuer le scellement du SVE
Post-élections	Archivage intermédiaire et définitif	Conserver sous scellés avant archivage

3.2.4 Description fonctionnelle du service attendu

Scrutins

Le scrutin désigne l'ensemble des opérations de vote et des modes de calcul destinés à départager les candidats aux élections.

Les modes de scrutins sont de différents types :

- Scrutin plurinominal majoritaire à 1 ou plusieurs tours.

- Scrutin de liste ou de sigle à la représentation proportionnelle à la plus forte moyenne ou au plus fort reste.

Les électeurs peuvent participer aux scrutins :

Depuis les locaux du CNRS, l'électeur ayant la possibilité de voter à partir de son poste de travail ou bien, s'il n'en est pas doté ou selon sa préférence, à partir d'un poste installé dans un espace électoral aménagé pendant les horaires de bureau pour la tenue des scrutins.

À distance, l'électeur a la possibilité de voter sur tout type de support dès lors qu'il dispose d'un accès à Internet.

Compte tenu du niveau d'équipement en postes de travail des agents du CNRS, le vote par Internet est à même de faciliter leur expression.

Électorat

La population électorale s'apprécie en fonction de chaque élection spécifique et le nombre d'électeurs varie d'une élection à l'autre.

Le corps électoral est constitué d'électeurs inscrits par CARE-CNRS lors de la constitution d'une liste électorale provisoire ou inscrits à leur demande.

Le corps électoral se compose des personnels CNRS et de personnels non CNRS présents au sein des unités en partenariat.

Au titre des élections organisées par le CNRS, le nombre d'électeur varie entre 27 000 et 72 000 électeurs environ. Ces chiffres sont indicatifs et n'engagent pas contractuellement le CNRS sur un minimum ou maximum.

L'élaboration de la liste électorale et sa conformité aux textes en vigueur relève de la seule responsabilité du CNRS.

Le titulaire est responsable de la vérification de l'intégrité de la liste et de sa bonne intégration dans le SVE.

Candidature

En fonction de l'élection concernée, les candidatures sont rattachées soit à une liste, soit à un sigle ou sont individuelles. Chaque liste ou candidature peut être accompagnée d'une profession de foi et/ou d'un CV.

Pour chaque scrutin, le CARE-CNRS précise le nombre exact de listes candidates ou de candidatures individuelles pour la personnalisation de l'écran de vote.

L'élaboration de la liste des candidats et sa conformité aux textes en vigueur relève de la seule responsabilité du CNRS.

Le titulaire est responsable de la vérification de l'intégrité de la liste et de sa bonne intégration dans le SVE.

Calendrier des opérations électorales

Le calendrier prévisionnel des opérations électorales 2027 figure à titre informatif et non contractuel en Annexe 6.5.

Le calendrier définitif et contractuel est arrêté entre le CARE-CNRS et le titulaire, lors de la réunion de démarrage pour l'élection concernée.

Modalités de vote

Le vote est à bulletin secret. Le vote électronique par internet constitue la modalité exclusive d'expression des suffrages.

Les dépouillements s'effectuent à la date définie entre le CARE-CNRS et le titulaire lors de la réunion de démarrage de chaque opération.

Éléments des précédents scrutins :

	CNESER	Conseil scientifique	Conseils scientifiques d'institut
Mode de scrutin	Scrutin de liste à la représentation proportionnelle au plus fort reste	Au scrutin plurinominal pour les électeurs des collèges A1, A2, B1 et B2. Au scrutin de liste à la représentation proportionnelle et à la plus forte moyenne pour les électeurs du collège C.	Au scrutin plurinominal pour les électeurs des collèges A1, A2, B1 et B2. Au scrutin de liste à la représentation proportionnelle et à la plus forte moyenne pour les électeurs du collège C.
Electeurs et électrices	31257	77191	77191
Listes candidates ou de candidats	7 listes dans le collège chercheurs 7 listes dans le collège IT	6 listes d'OS	5 listes d'OS par instituts soit 50 listes
Sièges à pourvoir	6 représentants au titre du collège chercheurs 4 représentants au titre du collège ingénieurs et techniciens	11 membres à élire : - 3 membres élus par les personnels relevant du collège A1, - 2 membres élus par les personnels relevant du collège A2, - 2 membres élus par les personnels relevant du collège B1, - 2 membres élus par les personnels relevant du collège B2, - 2 membres élus par les personnels relevant du collège C.	**12 membres élus répartis comme suit :** - 3 membres élus, par les personnels relevant du collège A1, - 2 membres élus, par les personnels relevant du collège A2, - 2 membres élus, par les personnels relevant du collège B1, - 2 membres élus, par les personnels relevant du collège B2, - 3 membres élus, par les personnels relevant du collège C.
Taux de participation	10,50 % pour collège CH 11,54 pour le collège IT	14,76%	14,76%

Une fiche détaillée présentant les différents scrutins 2027 est présentée au 6.3 ci-dessous.

Le bureau de vote électronique (BVE)

Chaque scrutin donne lieu à la constitution d'un BVE chargé des opérations suivantes :

- Avant le début du scrutin :
  - Procéder à la répartition des clés de chiffrement ;
  - Vérifier que les composantes du système de vote électronique ayant fait l'objet d'une expertise n'ont pas été modifiées et s'assurer que les tests prévus ont été effectués ;
  - Vérifier, pour chacun des scrutins, que l'urne électronique est vide, scellée et chiffrée par des clés de chiffrement délivrées à cet effet ;

- Procéder, pour chacun des scrutins, au scellement du système de vote électronique, de la liste des candidats, de la liste des électeurs, des heures d'ouverture et de fermeture du vote ainsi que du système de dépouillement.

- Pendant le scrutin :
  - Surveillance et contrôle régulier de son déroulement ;
  - Consultation notamment du taux de participation et de la liste d'émargement.

- À la clôture du scrutin, conduire les opérations post-électorales :
  - Scellement puis déchiffrement avant dépouillement ;
  - Dépouillement, validation (PV) et scellement des résultats après clôture du dépouillement.

À titre indicatif, chaque BVE comprend les membres suivants : un.e président.e et un.e secrétaire désigné.es par l'administration ainsi qu'un.e délégué.e de liste par organisation syndicale candidate au scrutin. Le délégué de liste peut se faire représenter par un suppléant.

La cellule d'assistance technique

Pour veiller au bon fonctionnement et à la surveillance du système de vote électronique, une cellule d'assistance technique est mise en place. Elle est compétente pour l'ensemble des scrutins.

Pendant le scrutin, le BVE est préalablement informé des demandes d'interventions techniques sur le système informatique de vote ainsi que des mesures envisagées pour remédier au dysfonctionnement.

Après accord du BVE, les interventions sur le système informatique de vote sont réservées aux seules personnes chargées de la gestion et de la maintenance appartenant à la cellule d'assistance technique et ne peuvent avoir lieu qu'en cas de risque d'altération des données.

Cette cellule comprend :

- des représentants du CNRS,
- des représentants du titulaire. Le nombre, la qualité et la disponibilité des représentants du titulaire doit permettre de garantir la bonne réalisation des missions assurées par la cellule tout au long des opérations électorales.

Le titulaire propose au CNRS pour validation un mode d'organisation, de collaboration et de suivi avec les représentants du CNRS membre de la cellule et le BVE.

Expertise indépendante

Préalablement à la mise en place ou à toute modification substantielle de sa conception, le SVE fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties légales et réglementaires.

Conformément à la réglementation, une vérification préalable de la conformité aux exigences de la CNIL et du niveau de sécurité offert pour le vote est effectuée sous la responsabilité d'un expert du domaine, indépendant, mandaté par le CNRS.

L'expertise doit inclure :

- Un audit des configurations en place
- Une prise d'empreinte
- Des tests d'intrusion
- Des tests de charge des systèmes

L'expertise couvre l'intégralité du dispositif installé avant le scrutin, y compris les conditions d'utilisation du poste dédié à cette expertise installé dans les services du CNRS, les conditions d'utilisation du système de vote durant le scrutin ainsi que les étapes postérieures au vote.

Le rapport de l'expert, mandaté par le CNRS, est transmis à la CNIL et aux organisations syndicales.

Il est attendu du titulaire qu'il prenne en compte les recommandations de l'expert au niveau du SVE afin que le processus électoral puisse se dérouler en conformité avec la réglementation en vigueur et les recommandations de la CNIL.

En cas de modifications apportées ultérieurement au système de vote par Internet, l'expert indépendant sera conduit à effectuer un audit complémentaire dans des conditions analogues.

En outre, dans la perspective éventuelle de réclamations, le CNRS peut être conduit à mandater l'expert indépendant pour opérer un certain nombre de vérifications notamment :

- En amont de l'élection,
  - Sur le contrôle de la conformité des référentiels électoraux pris en compte (scrutins, listes électorales, candidatures) ;
  - Sur le scellement du système de vote avant le scrutin ;
  - Sur le bon fonctionnement de l'ensemble de la chaîne de vote et de restitution des résultats (test préalable, cf. article 11, I. du décret n° 2011-595 du 26 mai 2011) ;
- À l'issue de l'élection,
  - Sur le bon déroulement du dépouillement des votes ;
  - Sur l'arrêt et le scellement définitif du système de vote ;
  - Sur le dispositif de conservation des données.

Dans le cadre des audits et des vérifications ponctuelles, l'expert indépendant sera conduit à :

- Planifier des réunions avec le titulaire ;
- Se rendre sur le site de la plate-forme d'hébergement du système de vote.

Dans le cadre des prestations, il est attendu du titulaire qu'il apporte son entier et plein concours à l'expert indépendant dans la conduite de ses opérations de vérification et qu'il l'assiste en tant que de besoin.

Par ailleurs, il est attendu du titulaire qu'il prenne en compte les recommandations de l'expert au niveau du système afin que le processus électoral puisse se dérouler en conformité avec la réglementation en vigueur et les recommandations de la CNIL.

3.2.5 Fonctionnalités attendues du système ou cas d'utilisation

3.2.5.1 *Intégration des listes*

Prise en charge sécurisée des listes électorales fournies par le CNRS

Les listes électorales peuvent être constituées par le CNRS sous forme de fichier dans un format préconisé par le RGI (Référentiel général d'interopérabilité) tels que csv, tsv etc…. Elles comportent les informations nominatives des agents du CNRS ou non CNRS ayant la qualité pour participer à l'élection envisagée.

Ces fichiers comportent à minima : l'identifiant électeur sur la liste électorale, civilité, nom, prénom, adresse professionnelle, mail professionnel, collège, grade.

Ces listes sont mises à jour à chaque nouveau scrutin.

Pour chaque scrutin, le CNRS transmet la liste électorale au titulaire à une date fixée lors de la réunion de démarrage de l'élection (de manière cryptée, les modalités précises de transmissions seront définies au démarrage du marché) afin de permettre la constitution du « fichier électeurs ».

Le titulaire doit mettre en place un processus d'échange sécurisé des informations et données relatives au « fichier électeur ». Le titulaire met en œuvre tous les moyens nécessaires pour assurer la confidentialité de ces données et en limiter la consultation aux seules personnes habilitées dans le cadre du projet.

Le fichier « électeurs » est transmis au titulaire aux seules fins suivantes :

- permettre l'attribution d'identifiants d'accès au SVE pour chaque électeur autorisé
- contrôler les accès au SVE
- enregistrer les émargements électroniques après chaque vote et assurer l'unicité du vote pour chaque électeur
- éditer les listes d'émargements

Le titulaire s'engage à l'expiration des délais de recours ou lorsqu'une décision juridictionnelle est devenue définitive, à détruire ces données sur demande du CNRS. Un procès-verbal de destruction sera adressé au CNRS.

Intégration et contrôle des listes intégrées

Le titulaire intègre ou permet d'intégrer dans le SVE les listes électorales, les listes des candidats, les listes des membres des bureaux de votes, les listes des délégués de liste.

À l'issue de l'intégration des listes dans sa base de données, le titulaire doit fournir les listes intégrées (export complet) ainsi que la liste des rejets, anomalies, doublons constatés.

Le titulaire contrôle et garantit la cohérence des fichiers (présence de données pour chaque électeur, ordre des listes telles que précisées par le CNRS).

Afin de permettre une vérification par le CNRS, le titulaire fournit au CNRS à l'issue de la génération et de la fourniture des identifiants, une liste de contrôle permettant de vérifier que tous les électeurs ont été pris en compte. . La forme et le contenu de cette liste sont définis d'un commun accord entre le CNRS et le titulaire.

Le SVE retenu doit permettre d'exporter les listes dans une version imprimable pour être affichées dans les locaux du CNRS conformément aux dispositions des décisions internes d'organisation de modalités des élections.

Pour information, le CNRS permet la consultation en ligne de la liste électorale (sur l'intranet CNRS). Elle n'est ouverte pour un scrutin donné qu'aux électeurs devant prendre part au scrutin et aux organisations syndicales ayant déposé une candidature à ce scrutin.

Intégration des professions de foi, logos et CV

Chaque candidature ou chaque liste de candidats peut s'accompagner de profession de foi (PF) des candidats et des CV le cas échéant.

Les professions de foi sont intégrées dans l'outil dans un format préconisé par le RGI (ce format et moyen technique seront à préciser au démarrage du marché).

Chaque électeur peut visualiser l'ensemble des professions de foi des candidats ou des listes de candidats. Les PF sont présentées dans l'ordre du tirage au sort des candidats ou des listes de candidats, effectué par la commission électorale.

Les logos des organisations syndicales sont intégrés également dans un format préconisé par le RGI (format à définir au démarrage du marché).

Tous les logos apparaissent à l'écran au format identique en vertu du principe d'égalité entre les candidats. Les PF, CV et logos sont transmis au titulaire pour intégration ou intégrés directement dans l'outil par le CNRS à une date arrêtée avec le titulaire.

Traçabilité des listes intégrées

Le titulaire conserve la trace de l'historique des versions de l'ensemble des listes intégrées dans le logiciel de vote, et met à disposition du CNRS un fichier récapitulatif.

3.2.5.2 *Gestion des listes*

Gestion de la liste électorale

La gestion de la liste électorale a pour objet de fournir à chaque électeur, un numéro unique de référencement, des codes lui permettant d'exprimer son vote par voie électronique en garantissant l'unicité et l'anonymat du vote et l'édition de la liste d'émargement.

La liste électorale peut, à la demande du CNRS, être modifiée jusqu'à la veille du premier jour du scrutin en cas d'acquisition ou de perte de la qualité d'électeur d'un agent.

Gestion de la liste de candidature ou des candidats

Selon le scrutin concerné, le CNRS adresse au titulaire des candidatures individuelles ou des listes de candidats.

Les listes mentionnent notamment : l'identifiant électeur sur la liste électorale, civilité, nom, prénom et, selon le scrutin nom de la liste et le logo, numéro d'ordre de présentation de la liste, numéro d'ordre de présentation des candidats sur la liste, nom de l'organisation syndicale, la section et le collège de vote

Le titulaire les intègre dans le système de vote électronique et s'assure que le candidat est présent dans le fichier électeur. Les listes sont présentées sur les écrans dans l'ordre défini par le CNRS.

Le titulaire veille à ce que la dimension des bulletins et la typographie soient identiques pour toutes les listes et permettent leur affichage sur une page d'écran unique.

Le titulaire met en œuvre une procédure de test permettant au CNRS de vérifier l'exactitude des listes de candidats soumises aux choix des électeurs ainsi que la présence des professions de foi et logos fournis. Pour certains scrutins, un curriculum vitae des candidats peut être intégré dans le SVE.

Gestion de la liste des membres du BVE et des délégués de liste

En vertu du cadre réglementaire il est constitué un BV / une commission électorale pour chaque scrutin. La composition de la liste des membres doit être implémentée sur la plateforme.

Chaque organisation syndicale ayant présenté des candidats désigne un délégué de liste et un suppléant pour participer au déroulement des opérations électorales.

La liste de ces délégués est transmise au titulaire ou intégrés directement dans l'outil par le CNRS au plus tard à une date fixée lors de la réunion de démarrage.

3.2.5.3 *Envoi de mail aux électeurs*

Gestion des courriers aux électeurs

Le titulaire assure la réalisation et la diffusion des différents mails vers les électeurs après validation au préalable du CARE-CNRS via un Bon à tirer (BAT) dématérialisé

Envoi de la notice explicative du Vote électronique

Le titulaire est chargé de rédiger une notice explicative claire qui précise les règles de fonctionnement du vote électronique. La notice est personnalisée selon la charte graphique en cours du CNRS.

Le titulaire établit une maquette que le CNRS valide avant l'envoi aux électeurs.

Cette notice est adressée pour chaque scrutin selon les modalités définies avec le titulaire lors de la réunion de démarrage du projet.

Elle doit être reçue par les électeurs au plus tard 15 jours ouvrés avant le début du scrutin.

En cas de perte ou de non-réception de sa notice de vote, un électeur peut demander, via la plateforme dédiée au scrutin, 10 jours ouvrés avant l'ouverture du scrutin et pendant toute la durée du scrutin et avant scellement de l'urne, une nouvelle émission de sa notice de vote, qui lui sera transmise par voie électronique. Le CNRS en est informé par le titulaire ou directement par le SVE.

La fonction de réassort est intégrée dans le SVE.

Ainsi, le SVE déclenche le réassort, qui consiste en les opérations suivantes :

Modification des infos concernant un électeur

- Désactivation des identifiants initialement attribués à l'électeur ;
- Génération d'une nouvelle notice de vote et de nouveaux identifiants pour l'électeur ;
- Vérification de l'adresse électronique de l'électeur ;
- Envoi de la notice de vote et des nouveaux identifiants à l'adresse électronique indiquée.

De même, pour l'ajout d'un électeur, le CNRS adresse au titulaire ou directement dans l'outil une demande de réassort.

Envoi des identifiants aux électeurs

Le titulaire sera chargé des modalités de génération et d'envoi des codes personnels selon les modalités définies avec le CNRS, conçues de façon à garantir leur confidentialité.

Les identifiants sont envoyés par le titulaire de façon à être reçus par les électeurs au plus tard 15 jours ouvrés avant l'ouverture du scrutin.

En cas de non réception ou de perte des identifiants, les électeurs peuvent demander en se connectant sur le site dédié au scrutin 10 jours ouvrés avant l'ouverture du scrutin et pendant toute la durée du scrutin et avant le scellement de l'urne de nouveaux identifiants, qui leur seront transmis par voie électronique. Le CNRS en sera informé par le titulaire.

La fonction de réassort fait partie du SVE.

Le SVE de réassort vérifie :

- L'identité de l'électeur ;
- Son inscription sur la liste électorale ;
- Son courriel ;

Après vérification de ces éléments en lien avec le CNRS, le SVE déclenche le réassort, qui consiste en les opérations suivantes :

Modification des infos concernant un électeur

- Désactivation des identifiants initialement attribués à l'électeur ;
- Génération de nouveaux identifiants pour l'électeur ;

- Vérification de l'adresse électronique professionnelle de l'électeur ;
- Envoi des nouveaux identifiants à l'adresse électronique professionnelle indiquée.

En cas de modification de la liste électorale par l'ajout d'un électeur, le CNRS adresse au titulaire une demande de réassort.

3.2.5.4 *Organisation du scrutin*

Procédure de vote

Avant le début du scrutin, il est procédé en présence des membres du BVE à l'établissement et à la répartition des clés de chiffrement, attribuées selon les modalités fixées par la décision portant organisation du vote électronique au CNRS.

Les membres présents vérifient que l'urne est vide, scellée et chiffrée.

L'électeur doit pouvoir accéder sur un seul écran à l'ensemble des listes en présence ainsi qu'aux professions de foi et sigles des organisations syndicales.

Le système de vote doit permettre le vote blanc et sa comptabilisation.

Le système doit présenter une interface graphique claire, présentant à l'électeur les éléments de vote sans équivoque possible.

Notamment, les candidatures et listes de candidats doivent être très facilement identifiées.

Les confirmations de vote et d'émargement doivent apparaître de façon claire, en faisant si possible référence à des notions issues d'un processus classique.

Le système doit bien s'assurer qu'il demande les confirmations nécessaires à l'électeur, afin d'empêcher toute manipulation accidentelle ne reflétant pas la volonté de ce dernier.

À ce titre, sont donc exclus du périmètre du vote électronique les dispositifs de vote par codes-barres, par téléphonie ou SMS ou encore le recours aux machines à voter.

Une fois l'électeur identifié, le système de vote doit présenter l'ensemble des informations nécessaires au processus.

L'électeur ne doit en aucun cas avoir à se référer à un document externe. Le manuel d'utilisation ou tutoriel fourni dans la notice de vote est seulement une aide supplémentaire permettant de se familiariser par anticipation avec le système de vote.

Son usage ne saurait être obligatoire en cours de vote. L'interface du SVE doit être suffisamment intuitive pour qu'un utilisateur raisonnablement familier avec l'outil informatique puisse l'utiliser sans difficulté.

Le système doit interdire toute erreur de manipulation pouvant amener à une ouverture ou une clôture du scrutin en-dehors des dates et heures prévues, à une modification des candidatures et listes de candidats ou des listes électorales, à une publication de résultats partiels en cours de vote, à un dépouillement en dehors de la procédure publique prévue.

Validation du vote

L'électeur exprime son vote qui doit apparaître clairement à l'écran.

L'électeur doit pouvoir revenir sur son choix de vote avant validation.

L'électeur doit confirmer son choix pour l'enregistrement du bulletin dans l'urne électronique.

La validation par l'électeur rend le vote définitif et entraîne automatiquement l'émargement dans le fichier des électeurs, l'enregistrement du bulletin dans l'urne, la génération d'un accusé de réception.

L'électeur imprime ou reçoit un accusé de réception mentionnant le scrutin, la date et l'heure de l'enregistrement.

Le suffrage exprimé est anonyme et chiffré par le système.

Il est transmis au fichier « contenu de l'urne électronique » et conservé jusqu'au dépouillement et jusqu'au terme des délais de recours.

Clôture du vote

Le logiciel de vote se ferme automatiquement à l'heure fixée dans les décisions calendrier et modalités de vote du CNRS.

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 et la sécurité des données.

3.2.5.5 *Dépouillement et publication des résultats*

Scellement du vote

Le BVE contrôle, avant le dépouillement, le scellement du système.

Le BVE comprend un ou une président.e et un ou une secrétaire de séance (désignés par le P-DG du CNRS) ainsi que les délégués de liste.

Le BVE proclame la fermeture du scrutin et l'ouverture de la procédure de dépouillement.

Dépouillement du vote

Le Président du BVE et les délégués de liste autorisent le dépouillement.

Le dépouillement n'est possible qu'après l'activation des clés de chiffrement fournies par le titulaire.

Le décompte des voix apparaît lisiblement à l'écran selon les modalités définies par le CNRS (voix obtenues par candidats, par listes de candidats, nombre de sièges par liste…), cette liste doit être exportable sous forme de fichier.

Le BVE contrôle que la somme des suffrages exprimés et des votes blancs correspond au nombre de votants de la liste d'émargement électronique.

Publication des résultats et attribution des sièges

Le SVE édite les résultats de manière quasi-instantanée.

Les résultats sont affichés à l'écran pour les membres de la commission électorale.

Après la validation par la commission électorale le BVE procède à l'attribution des sièges.

Le Président du BVE rédige et signe le Procès-verbal de dépouillement. Il est signé par tous les membres du BVE.

3.2.5.6 *Clôture*

Fourniture de statistiques

Le titulaire s'engage à fournir sous forme de fichier dans un format préconisé par le RGI des statistiques telles que définies par le CNRS.

Clôture du vote et destruction des données

À l'issue du scrutin, le titulaire restitue au CNRS, tous les fichiers supports (copies des codes sources et exécutables des programmes et du système sous-jacent, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) qui doivent être conservés sous scellés jusqu'à l'épuisement des voies et délais de recours contentieux restant en sa possession et détruit toutes copies, totales ou partielles, qu'il a été amené à effectuer, sur quelque support que ce soit.

Le titulaire transmet au CNRS le Procès-verbal (PV) de destruction des données.

Conformément à la Délibération n° 2019-053, toutes les données traitées à l'occasion des scrutins doivent être conservées sous scellés jusqu'à l'épuisement des délais de recours contentieux.

Le CNRS convient que cette conservation sera assurée par ses propres moyens.

3.2.6 Communication des listes et professions de foi

Afin de permettre au CNRS de lui remettre les données et fichiers à intégrer au SVE, le titulaire mettra à sa disposition cette même plateforme sécurisée pour lui permettre de :

- lui remettre (format CSV) les fichiers d'initialisation des scrutins, des bureaux de vote, des équipes électorales, des listes électorales et des candidatures ou listes de candidats par scrutin.
- lui remettre les fichiers correspondant aux candidats ou listes de candidats et aux professions de foi au format PDF/A. De même, le CNRS remet les logos au format JPEG ou PNG.

3.3 EXIGENCES DE CONDUITE DU CHANGEMENT

3.3.1 Assistance à la conduite du changement

Le projet de mise en œuvre du vote électronique au CNRS donnera lieu à des réunions d'information diverses à l'attention des représentants des personnels (réunions techniques, groupes de travail, comités techniques…).

Au cours de ces différentes réunions, le titulaire mobilise les profils experts en capacité de répondre aux questions sur la solution technique et de sécurité déployée pour l'organisation des opérations électorales et de présenter un argumentaire relatif aux éléments saillants du dispositif de l'élection visant notamment à garantir le respect des principes fondamentaux qui commandent les opérations électorales (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).

3.3.2 Foire aux questions et tutoriel

Le titulaire initialise le contenu de la FAQ sous format électronique de type .doc et .pdf en tirant partie de son expérience dans l'organisation des élections. Par la suite, il apporte son expertise fonctionnelle et technique au CNRS pour enrichir la FAQ en fonction des questions complémentaires identifiées au cours du projet.

La FAQ a vocation par nature à offrir des réponses précises et concises aux interrogations les plus fréquentes de la part des électeurs, des membres des bureaux de vote et des représentants des organisations syndicales en phase pré-électorale, lors des scrutins puis en phase de dépouillement et de proclamation des résultats.

Ces questions peuvent avoir trait à l'accès à la plateforme, à la sécurité mise en place, à la prise en compte effective des votes lors des scrutins, etc.

Une version de la FAQ est mise en ligne sur les sites Intranet du CNRS.

Le titulaire élabore en concertation avec le CNRS notamment, un tutoriel au format pdf et un tutoriel animé respectant la charte graphique.

Il sera visible sur le site de vote en ligne du titulaire et sur l'intranet du CNRS.

3.3.3 Assistance Utilisateur et organisateurs des élections

Types d'assistance attendus

Bénéficiaire	Type	Modalités
Électeurs	Assistance à l'utilisation des services de vote électronique en cas de difficultés d'accès ou de vote (renvoi & initialisation des clés d'authentification, tutoriel en ligne, FAQ)	Assistance dématérialisée et accessible en ligne depuis le site d'accès au service de vote électronique du titulaire
Organisateurs des élections et membres de bureaux de vote électronique	Assistance lors de chaque scrutin pour les opérations dont le BVE est responsable Assistance en cas de dysfonctionnement de la plateforme Constaté par les organisateurs ou les électeurs	Modalités de formation au SVE Outils d'enregistrement et de suivi des demandes à détailler par le titulaire dans son offre

Assistance aux organisateurs des élections et au BVE

Le titulaire assure une assistance auprès du CARE-CNRS ou des membres de l'équipe projet.

Il s'agit de fournir des prestations :

- D'assistance attendue de la part du titulaire lors de l'ouverture du système de vote (élections à blanc, …) ;
- D'accompagnement complémentaire, selon les besoins du CNRS
- Un accompagnement sur site du BVE lors des opérations de génération des clés, de scellement/descellement, de tests préalables à l'ouverture du scrutin ou de dépouillement des votes,
- Une assistance au cours de l'ouverture du système de vote.

Les modalités et outils d'enregistrement et de suivi des demandes d'assistance émises par le CNRS sont précisées dans l'offre du titulaire.

Assistance aux électeurs

Il s'agit de fournir les prestations d'assistance au bénéfice des électeurs, en cas de difficultés rencontrées dans la connexion ou l'utilisation du système de vote.

Cette assistance doit inclure à minima la possibilité pour un électeur :

- D'initialiser ou de demander le renvoi des clés d'authentification, après vérification de l'identité de l'électeur ;
- De consulter le tutoriel en ligne ;
- De consulter la foire aux questions ;
- De bénéficier d'un centre d'appel téléphonique durant la période de vote.

Pour les autres demandes d'assistance, seuls les organisateurs des élections pourront les relayer auprès du titulaire dans le cadre de la prestation d'assistance aux organisateurs.

Le centre d'appel téléphonique

En application de l'article 8 du projet d'arrêté relatif aux modalités d'organisation du vote électronique, le CNRS doit mettre en place un centre d'appel chargé de répondre aux questions des électeurs pendant toute la période de vote et selon des modalités et des horaires fixés par la décision d'organisation du scrutin. Le titulaire met en place ce centre d'appel téléphonique pour le CNRS.

Ce centre d'appel est chargé d'assurer une assistance aux électeurs, de les aider à faire fonctionner le système sur leur ordinateur, tablette ou Smartphone en cas de difficulté technique, et de les diriger vers les services adéquats en cas de problème (problème de connexion ou d'authentification, demande de réassort...).

Le numéro est accessible (la diffusion sera assurée dans la notice de vote notamment) depuis la métropole, l'étranger et à l'outre-mer (DROM/COM).

Il s'agit d'un service gratuit pour l'appelant. Le centre d'appel est ouvert de 8h à 19h pendant toute la période de vote.

Le titulaire produit quotidiennement la liste récapitulative des incidents survenus à CARE-CNRS précise les dates et heures de la demande, de réponse et de résolution de l'incident.

3.3.4 Formations

Le titulaire est chargé de concevoir les modules de formation ainsi que de réaliser en présentiel les sessions de formation des équipes électorales.

Le titulaire élabore le plan de formation en collaboration avec le CNRS.

Le plan de formation expose les modalités de formation et précise l'organisation et le calendrier des actions de préparation, de dispense et d'évaluation des formations.

La formation est assurée en présentiel par des formateurs du titulaire pour les organisateurs de l'élection.

Le titulaire conçoit, réalise et met à jour les supports et outils nécessaires aux formations. Il doit communiquer les documents supports de formation au CNRS sous format électronique de type .doc et .pdf.

Cette formation recouvre en particulier les domaines suivants :

- Le cadre légal du vote électronique,
- Les principes du vote électronique,
- Les typologies des rôles à l'œuvre dans le vote électronique,
- Une sensibilisation à la sécurité et aux responsabilités inhérentes à l'utilisation du vote électronique adaptée aux différents profils des acteurs,
- La surveillance effective du scrutin électronique,
- Une formation à l'utilisation de l'outil pour chacun des rôles :
- Configuration d'un scrutin,
- Gestion des professions de foi,

- Ouverture du scrutin,
- Supervision / surveillance du scrutin,
- Clôture du scrutin,
- Dépouillement,
- Publication des résultats.

Cette formation doit s'accompagner d'un support de communication permettant aux agents formés d'être en capacité d'expliciter les processus de connexion au SVE et ceux relatifs au vote à l'ensemble des électeurs.

4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION

Les prestations doivent se conformer aux exigences, mentionnées ci-après, sur les aspects généraux, techniques et de sécurité.

Ces exigences s'imposent au titulaire sur tout le périmètre et toute la durée de sa prestation.

4.1 EXIGENCES D'INTÉGRATION DANS LE SI

Aucune intégration dans le SI du CNRS n'est envisagée.

4.2 EXIGENCES TECHNIQUES

4.2.1 Éléments techniques structurants

L'application est une application ouverte sur Internet et y compris aux dispositifs mobiles.

Elle est ouverte à environ 70 000 utilisateurs authentifiés au maximum, ce chiffre étant variable d'une élection à l'autre.

On estime cependant que, toutes populations confondues, la fréquentation de l'application est limitée à 5000 utilisateurs par jour.

Les fins de période de vote peuvent engendrer des pics de charge sur le service, celui-ci est capable de les absorber.

4.2.2 Engagements de qualité de service pour l'application

4.2.2.1 *Disponibilité*

Les scrutins organisés au titre du présent marché se déroulent en France métropolitaine, dans les DROM-COM et à l'étranger.

Le SVE doit permettre ce mode de fonctionnement et notamment :

- Le SVE doit inclure la gestion des fuseaux horaires de manière à indiquer pour chaque scrutin les heures locales d'ouverture, de fermeture, de vote, etc.
- Le système de vote électronique doit être accessible 7 jours sur 7, 24 heures sur 24, pendant la période du scrutin,

Le titulaire est tenu au respect des contraintes de disponibilité pendant la période allant de J-1 de la date d'ouverture du scrutin jusqu'au J+1 du dernier jour de dépouillement inclus.

Dans le cas d'un déploiement d'une nouvelle version (mise en production), elle doit se faire autant que possible en dehors des périodes de vote, et en tout état de cause, si une action était indispensable pendant un scrutin, elle se ferait dans le respect des SLA et des DMIA/RPO/RTO définis au présent cahier ces charges.

Les périodes de maintenance programmée se font à des périodes décidées en commun accord entre le CNRS et le titulaire.

4.2.2.2 *Intégrité*

La solution doit permettre un contrôle de l'intégrité des données (intégrité structurelle et intégrité du contenu).

En cas de corruption de données, la perte de données acceptable est nulle (RPO=0). Si nécessaire, l'application doit avoir la possibilité de reprendre les flux ou les batch qui auront été générés lors de la période de perte de données.

Le CNRS doit parfaitement maîtriser la nature des données utilisées par l'application et les mécanismes permettant de restaurer un jeu de données cohérent et exhaustif en cas de nécessité.

Le titulaire est tenu de fournir un descriptif exhaustif des données utilisées et des contraintes techniques associées à une restauration. L'usage des contraintes référentielles est fortement conseillé.

4.2.2.3 *Performances*

Le CNRS définit comme suit les caractéristiques de performances attendues de l'application :

- Connexion au serveur (contrôle des accès compris) et affichage de la page d'accueil en moins de 5 secondes.

- Temps d'affichage d'une IHM de saisie / consultation inférieur à 3s dans 80% des cas.
- Temps d'exécution d'une requête de recherche inférieur à 10 secondes,
- Temps de génération d'un état inférieur à 20 secondes.
- Capacité du SVE à accepter 50% des votants sur la première journée du vote

Ces chiffres correspondent à des transactions simples et largement utilisées dont le temps de réponse est mesuré sur le poste client hébergé sur le même réseau.

La plate-forme doit offrir une qualité de service garantie en termes performance et tenue de charge.

- Nombre simultané d'électeurs acceptés sans dégradation sensible des performances à hauteur de 30% du nombre total d'électeurs ;
- Le SVE est disponible avec, pour le premier et le dernier jour de scrutin, des pics de charge prévisibles.

Pour information, la capacité d'accès à Internet pour certaines représentations est limitée à 2 Mbps (ADSL)

Certaines fonctionnalités peuvent déroger à ces règles. Toutefois elles doivent :

- faire l'objet d'un accord explicite du chef de projet DSI,
- afficher à l'utilisateur des éléments permettant de juger de leur avancement.

Le titulaire fournit au CNRS :

- des éléments de dimensionnement de la plate-forme de production pour garantir un niveau de performance conforme au besoin en regard des éléments de volumétrie disponibles ;
- des éléments de tuning de la plate-forme permettant d'optimiser les performances (système, base de données, …).

Le titulaire fournit au CNRS en même temps que chaque version stable de l'application le rapport des tests de performances qui auront été menés.

Ce rapport met particulièrement en avant les éléments chiffrés concrets qui permettent de valider les temps de réponses exigés par le CNRS en condition de forte charge applicative. Il met aussi en évidence les composantes techniques de l'application nécessitant le plus de ressources techniques et induisant des temps de réponses significatifs.

4.3 EXIGENCES D'ERGONOMIE-GRAPHISME

Les applications Web du CNRS doivent répondre à des impératifs d'identité et d'ergonomie. Elles doivent également suivre des recommandations techniques pour leur intégration afin de satisfaire au mieux les exigences d'accessibilité auxquelles tous les services Web d'un établissement public doivent se conformer.

Elles doivent appliquer les règles décrites ci-dessous afin de respecter une cohésion intra et inter-applicative au sein du CNRS.

4.3.1 Règles d'ergonomie

L'application doit être ergonomique c'est-à-dire qu'elle doit être facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale.

L'application doit accompagner l'utilisateur qui doit savoir ce qu'il doit faire sur la page active. Il doit également pouvoir naviguer et se repérer dans l'ensemble de l'application. Pour cela, l'application doit utiliser les systèmes de navigation les plus adaptés, *par exemple : menus, onglets, enchaînements d'étapes, etc*.

Les éléments fonctionnels du cœur de page doivent être disposés de manière à permettre une lecture facile, avec des éléments regroupés et structurés.

La conception de l'IHM peut faire appel à des composants d'IHM innovants, *par exemple : effets de transition, de transparence, mouvements, auto complétion, etc*.

L'application doit être conçue de manière globale et homogène.

Référence	Libellé exigence	Priorité
ERG_006	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal.	1

Référence	Libellé exigence	Priorité
ERG_007	Les tableaux sont conçus de manière optimisée (utilisation de formules synthétiques, de pictogrammes, interlignages valorisés par des couleurs de fond, mise en valeur des entêtes, des liens, ordre des colonnes pertinent, système de navigation pour les tableaux longs).	1
ERG_008	Les titrailles et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).	1
ERG_009	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.	1
ERG_010	Dans le cas de solution responsive, l'interface est adaptée au pilotage de l'ihm via un doigt (zone cliquable agrandie, survol impossible, navigation par balayage de l'écran, etc.). Les textes sont agrandis.	1

4.4 EXIGENCES DE SÉCURITÉ

Le référentiel des exigences sécurité est présenté dans le tableau ci-dessous. Lorsque nécessaire, il est complété par des éléments détaillés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
SSI_101	Un dossier de sécurité pour la solution détaillant les mesures de sécurité opérationnelle mises en application, ainsi que tous les éléments de preuve de la réelle application de ces mesures (captures d'écran, fichiers de configuration, comptes rendus...) est créé et maintenu. Il indique également comment ces mesures sont régulièrement vérifiées et le dossier comprend le CR des vérifications, le compte-rendu des audits. Ce même dossier constitue une preuve de mise en œuvre des mesures de sécurité conformément au RGPD.	0
SSI_102	Lorsque des fonctions de visa ou de signature électronique sont mises en œuvre, elles respectent les dispositions du règlement eIDAS (https://cyber.gouv.fr/le-reglement-eidas-n9102014) et du RGS (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs). La mise en œuvre est obligatoirement discutée avec le département Cybersécurité.	0
SSI_103	Les environnements hors production (développement, essai, recette, école, pré-production, formation, etc.) n'utilisent pas les données et accès de production.	0
SSI_CRYPT_101	Seuls des protocoles de transport de données chiffrés sont utilisés. Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents	0
SSI_PDI_101	Un inventaire des ressources matérielles et logicielles composant la solution et de leurs versions est maintenu à jour.	0
SSI_021	Le datacenter hébergeant la solution ainsi que les équipes d'exploitation doivent être localisés dans l'Union Européenne. De plus, les données ne devront pas être hébergées sur un environnement soumis à des lois extraterritoriales (comme par exemple le CLOUD ACT). Un hébergement souverain qualifié SecNumCloud est attendu (ou norme Européenne de portée équivalente).	0
SSI_022	Le titulaire et ses éventuels sous-traitants sont certifiés ISO27001 (ou équivalent) pour leur domaine d'intervention respectif dans le cadre du présent marché, ou démontrent qu'une démarche dans ce sens est en cours. Dans le premier cas, il produit la déclaration d'applicabilité (DdA) complète précisant le périmètre.	1
SSI_023	Le titulaire propose au pouvoir adjudicateur un Plan d'Assurance Sécurité (PAS)	0
SSI_024	Le titulaire dispose d'un plan de reprise et/ou de continuité d'activité. Il est fourni à l'appui de l'offre si disponible et communicable.	0

4.4.1 Auditabilité

Niveau de traçabilité

La solution met en œuvre obligatoirement la politique de traçabilité de l'ensemble des accès (autorisés et refusés) et des opérations réalisées. Ces traces doivent contenir à minima les informations suivantes :

- Date et heure de l'accès (avec une information d'horodatage fiable) : connexion et déconnexion ;
- Compte d'accès ;
- Etat de l'accès : autorisé ou refusé (et la raison en cas d'échec) ;
- Opérations réalisées ;
- Adresse IP source et protocole d'accès.

De plus, la solution doit implémenter ces fonctions autour de la gestion des traces :

- Durée de rétention des traces (mécanisme de rotation des traces, capacité de rétention maximale) ;
- Centralisation des traces ;
- Sauvegarde des traces ;
- Archivage des traces ;
- Protection des traces (pour assurer leur disponibilité, intégrité et confidentialité) ;
- Supervision des traces.

Gestion des traces

La solution doit permettre un reporting sur les :

- Opérations en général ;
- Accès et les opérations qualifiées comme sensibles réalisées ;
- Sorties d'informations (ou exports de données);
- Données non intègres.

L'accès à ces rapports doit être réservé aux personnes clairement identifiées et habilitées.

5 CADRE D'ORGANISATION DES PRESTATIONS

5.1 SYSTÈME QUALITÉ

En ce qui concerne la qualité, le CNRS préconise de s'appuyer sur la norme ISO 9001 (Systèmes de management de la qualité) et sur des référentiels de bonnes pratiques tels que ITIL® : Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library).

Le CNRS est particulièrement attentif à la forte orientation utilisateur, l'approche processus et l'amélioration continue.

Si le cas est prévu, les dispositions qualité (processus, organisation, méthodes, outillage…) nécessaires au développement spécifique de l'outil et à la bonne exécution de toutes les prestations définies dans l'accord-cadre sont explicitées.

5.2 ORGANISATION DES ÉQUIPES PROJET

5.2.1 Organisation de l'équipe projet CNRS

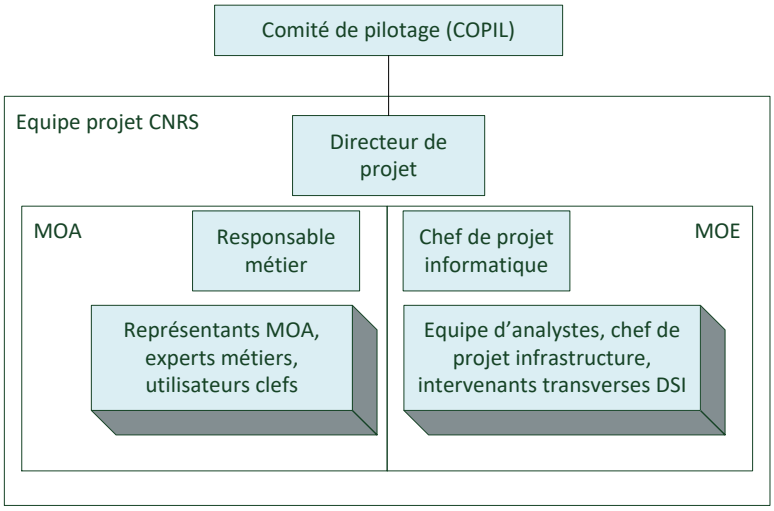


Figure 1 : Organisation du projet au CNRS

La composition de l'équipe projet CNRS est la suivante :

- un **directeur de projet** appartenant à la DAJ ;
- un **chef de projet informatique** appartenant à la DSI ;
- un **responsable métier** appartenant à la DAJ ;
- une **équipe projet maîtrise d'ouvrage (MOA)** : DAJ, intervenants de CARE-CNRS ;
- une **équipe projet maîtrise d'œuvre (MOE)** : équipe projet e-vote de la DSI, dont un **chef de projet infrastructure**.

Le directeur de projet pilote, coordonne et suit globalement l'avancement de l'ensemble du projet.

Côté maîtrise d'ouvrage, le responsable métier s'appuie sur des représentants des différentes MOA, des experts métier et des utilisateurs, pour définir les besoins métier, les prioriser, valider la solution fonctionnellement et mettre en œuvre la conduite du changement.

Côté maîtrise d'œuvre et au besoin, le chef de projet informatique s'appuie sur une équipe d'analystes dédiée au projet et sur des équipes transverses à la DSI (urbanisation, EAI, sécurité, qualité-méthodes, graphisme…).

L'interlocuteur CNRS privilégié du titulaire pour les relations contractuelles est le chef de projet informatique.

Un **comité de pilotage** (interne CNRS) assure le pilotage stratégique du projet. Il est composé des directions assurant la maîtrise d'ouvrage du projet, de la maîtrise d'œuvre (DSI).

5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire

Le titulaire met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre. Il identifie les compétences nécessaires et s'assure du maintien de ces compétences tout au long de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_009	Le titulaire s'engage sur une équipe ferme pour le démarrage de l'accord-cadre, a minima pour les profils types de chef de projet et responsable technique.	1
QUA_013	Le titulaire met en œuvre des dispositions pour gérer la variation de charges de son équipe afin de garantir sa flexibilité et sa réactivité en fonction de l'activité du projet.	1

5.3 DISPOSITIFS DE CONDUITE DE PROJET

5.3.1 Structures de pilotage projet

Le titulaire propose des structures de pilotage adaptées au contexte du projet.

Référence	Libellé exigence	Priorité
QUA_016	Le titulaire fournit aux participants des comités un document support dans les deux jours ouvrés précédant la réunion.	1
QUA_017	Le titulaire rédige et adresse le compte-rendu des comités aux participants dans les deux jours ouvrés consécutifs au comité.	0
QUA_018	Le titulaire propose et met en œuvre des structures de pilotage adaptées à la méthode de développement du projet.	1

5.3.2 Pratiques de gestion de projet

Le CNRS souhaite qu'a minima le titulaire mette en œuvre les pratiques de gestion de projet suivantes :

Référence	Libellé exigence	Priorité
QUA_021	Chaque courriel envoyé suit les préconisations suivantes : ▪ préfixer l'objet du message avec le nom du projet : « [Nom projet] sujet » ; ▪ si nécessaire, indiquer l'urgence attendue pour la réponse en précisant URGENT dans l'objet du message « [nom-projet] URGENT sujet » ; ▪ dans le corps du message, préciser ce qui est attendu du destinataire : simple information, avis, décision, action… Si nécessaire, indiquer la date d'échéance attendue pour la réponse ; ▪ éviter les pièces jointes, les remplacer par des liens vers l'outil collaboratif du CNRS.	1
QUA_022	Le titulaire suit et informe le CNRS des actions identifiées lors des comités ou réunions diverses avec le CNRS.	1
QUA_024	Le titulaire gère les risques du projet qui ont été formalisés dans son offre et ajustés lors du démarrage et tout au long de l'accord-cadre.	1
QUA_025	Le titulaire définit les procédures d'alertes et d'arbitrage. Le titulaire adapte ces procédures en fonction de la méthode de développement du projet.	1
QUA_026	Le titulaire met en œuvre une procédure de gestion de crise en cas d'alerte avérée. Il précise le processus d'escalade suivi pour le traitement et la résolution de ces problèmes.	1

La gestion de crise s'impose dans le cas d'incident persistant (délai de résolution indéterminable, correction impossible ou inefficace), d'incident de sécurité de grande envergure (attaque virale), d'incidents multiples, de risque d'altération de données (perte de sauvegarde, …), de risque avéré sur le fonctionnement et les missions du CNRS (atteinte à l'image de marque), et de l'occurrence de tout événement à caractère improbable ou de criticité catastrophique (atteinte à la sauvegarde des personnes ou des biens).

5.3.3 Indicateurs de pilotage et qualité du projet

Le titulaire propose des indicateurs pertinents et adaptés au contexte du projet.

5.3.4 Activités de recette (à la charge du CNRS)

La recette CNRS est composée de tests métier (par les maîtrises d'ouvrage).

Les anomalies détectées par le CNRS sont formalisées et classifiées selon 3 niveaux de gravité (cf. glossaire du Livret 2 du CCTP) dans l'outil de gestion des anomalies et évolutions du CNRS.

Référence	Libellé exigence	Priorité
QUA_039	Le titulaire s'engage à corriger la totalité des anomalies issues de la recette avant mise en production, sauf dérogation explicite du CNRS.	0

5.4 GESTION DES ENVIRONNEMENTS

5.4.1 Environnements

- Le titulaire fournit et administre l'ensemble des plates-formes serveurs du projet

Le titulaire est responsable (installation et exploitation) des composants d'infrastructures, OS, stockage, réseau, sur tous les environnements.

5.5 GESTION DE LA DOCUMENTATION

La documentation produite par le titulaire doit être de qualité et permettre une bonne compréhension des mécanismes développés à des fins d'exploitation et de maintenabilité.

Référence	Libellé exigence	Priorité
QUA_047	Tous les documents produits dans le cadre du présent accord-cadre sont livrés sous format électronique modifiable (donc pas uniquement en pdf).	1
QUA_048	Les documents du projet sont déposés et partagés par le CNRS et le titulaire dans l'outil collaboratif du CNRS.	1

Les principes de gestion de la documentation préconisés au CNRS sont les suivants :

Référence	Libellé exigence	Priorité
QUA_050	Tout document produit contient : le nom du document, une référence, la date de dernière mise à jour, la version, l'historique des versions (si besoin), le sommaire, les pages numérotées, les marques de révision apparentes d'une version à l'autre (si besoin).	0
QUA_051	Chaque document reçoit une référence unique au sein du projet (nom du fichier) : **Nom-du-projet_Identification-du-document_[Confidentialité_]Vx.y** **ou** **Nom-du-projet_Identification-du-document_[Confidentialité_]Date-evenement** avec **:** ▪ Identification-du-document = nom représentatif du contenu, de la forme : Type-document_[Code-domaine]_Libelle-libre ▪ Confidentialité : code indiquant le niveau de confidentialité du document, DL, DC ou DR ▪ Vx.y : version du document pour les documents de référence ▪ Date-evenement au format AAAAMMJJ pour les documents événementiels (CR de réunion…). La référence du document ne contient aucun caractère accentué ni espace (à remplacer par « - »).	1

Référence	Libellé exigence	Priorité
QUA_052	Chaque document mentionne dans sa référence le code de confidentialité. Seuls les documents de niveau classification PUBLIC (cible de diffusion non contrôlée : la publication de l'information présente un impact nul pour l'organisme) n'ont pas de code de classification. Les différents codes et niveaux de classification sont les suivants : ▪ **DL** :DIFFUSION LIMITEE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ; ▪ **DC** : DIFFUSION CONFIDENTIELLE pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important ; ▪ **DR** :DIFFUSION RESTREINTE conformément à l'II901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique.	1
QUA_053	Pour chaque document, un marquage est apposé afin de signifier le niveau de protection et les mesures réglementaires à appliquer en ce qui concerne la communication, la diffusion, la reproduction, la conservation et la destruction de ceux-ci : le niveau de classification (DIFFUSION LIMITEE, DIFFUSION CONFIDENTIELLE ou DIFFUSION RESTREINTE) est apposé en haut de chaque page en caractères gras, rouge et en capitales.	1
QUA_054	Le numéro de version du document est incrémenté à chaque modification du contenu du document devant faire l'objet d'une diffusion (il n'est pas incrémenté pour des corrections portant sur la forme du document - fautes de frappe, d'orthographe, ...). Le numéro de version est de la forme : x.y, avec : ▪ **x** : incrémenté à chaque évolution majeure du document (*par exemple*, ajout de chapitres, changement de version de l'application, refonte du document…) ▪ **y** : incrémenté à chaque évolution mineure (*par exemple, prise en compte de remarques de relecture, ajout de précisions*…).	1

Le CNRS formalise ses remarques au travers d'une fiche de relecture pour les documents qui ont fait l'objet d'une livraison, par marques de révision dans le document pour les comptes rendus et les mises à dispositions intermédiaires.

Les règles et pratiques à mettre en œuvre autour de la gestion documentaire sont ajustées d'un commun accord au démarrage de l'accord-cadre.

5.6 MESURES ET CLAUSES DE SÉCURITÉ

5.6.1 Gestion de la Sécurité par le titulaire

La Solution de Vote doit respecter a minima l'intégralité des recommandations du niveau 2 du guide de l'ANSSI *recommandation pour la mise en œuvre du vote par Internet pour les élections non politiques [ANSSI-PA-118, 2026-04-24),* dont sont extraites les mesures suivantes.

Si toutes les mesures ne sont implémentées à date de la réponse, le titulaire doit fournir son plan de mise en conformité sur le référentiel *ANSSI-PA-118, 2026-04-24,* avec comme date cible au plus tard le début des campagnes de vote CNRS.

Le titulaire doit fournir un rapport d'expertise indépendante de sécurité, ou l'attestation de conformité accompagnée de sa synthèse exécutive satisfaisant aux conditions suivantes :

- Réalisée par un tiers indépendant qualifié PASSI par l'ANSSI.
- Portant de manière explicite sur la version exacte du Système de vote qui sera déployé dans le présent marché.
- Daté de moins de deux ans à la date de remise des offres ou mis à jour à la suite de la dernière évolution majeure de l'application.

- Concluant à l'absence de réserves majeure ou critique bloquante au regard des exigences du niveau 2 de l'ANSSI.

N°	Exigence	Priorité
	Mesures liées à la gouvernance et au maintien en condition de sécurité	
R-01	Le prestataire doit fournir des procédures détaillées, notamment pour le déploiement, l'utilisation et la surveillance du système, par le bureau électoral, pour la tenue des cérémonies ou pour la gestion des supports contenant des clés cryptographiques (1-08). Ces procédures doivent être revues par l'expert indépendant, au sens de la délibération de la CNIL [Délibération n° 2026-045 du 19 mars 2026 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique et abrogeant les délibérations n° 2010-371 du 21 octobre 2010 et n° 2019-053 du 25 avril 2019.]. Une fois revues et stabilisées, ces procédures doivent être respectées par l'ensemble des acteurs impliqués, notamment l'organisateur du scrutin et le prestataire, et tout écart doit être identifié	0
R-02	L'organisateur du scrutin doit identifier et analyser les développements spécifiques à ajouter à la solution de vote standard proposée par le prestataire. Si une analyse de risque est réalisée, elle doit tenir compte de ces développements.	0
R-04	Le prestataire doit réaliser une cartographie de l'ensemble des composants techniques du système de vote. La cartographie doit couvrir au minimum les équipements réseaux, les moyens de communication externes, les équipements de sécurité, les logiciels d'infrastructure, les composants logiciels tiers, les bases de données, les serveurs, leurs systèmes d'exploitation, les solutions de virtualisation, et les supports de stockage.	0
R-05	Le prestataire de vote doit utiliser les dernières versions stables (incluant les correctifs de sécurité) des composants du système de vote, tels que cartographiés. Considérant le système de scoring CVSS [Common Vulnerability Scoring System SIG., https://www.first.org/cvss/], il est recommandé que tous les composants du système de vote, ainsi que leurs dépendances, ne contiennent aucune faille publique de criticité supérieure ou égale à medium. De même, il est recommandé que tous les composants du système de vote exposés sur Internet ne contiennent aucune faille publique de criticité supérieure ou égale à low. Cela inclut notamment les terminaisons TLS exposées aux électeurs et le client de vote.	0
R-54	Il est demandé que le prestataire suive les bonnes pratiques pour développer le système de vote, telles que les Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur [Guide ANSSI-PA-009 v2.1, ANSSI, avril 2021.] de l'ANSSI et les recommandations du TOP 10 OWASP [https://owasp.org/Top10.].	0
R-06	Le système de vote doit être audité, notamment sur les points suivants : • Les versions des composants du système de vote. • La correction des failles de sécurité. • La conformité des mécanismes cryptographiques aux Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques [18]. • La conformité des mécanismes d'authentification des électeurs, en particulier lors du transfert des secrets à des sous-traitants (1-03). • La conformité des liaisons TLS (1-05). • Le développement, le durcissement, l'administration et la sécurité physique du système de vote (2-06). • Sur demande de l'organisateur du scrutin, la conformité au cahier des charges du projet. L'audit doit être réalisé en conformité avec les recommandations de la CNIL (Délibération n° 2026-045 du 19 mars 2026 portant adoption d'une	0

N°	Exigence	Priorité
	recommandation relative à la sécurité des systèmes de vote par correspondance électronique et abrogeant les délibérations n° 2010-371 du 21 octobre 2010 et n° 2019-053 du 25 avril 2019.) : pour chaque scrutin de niveau 3, et éventuellement en réutilisant des expertises réalisées dans les 12 derniers mois pour les scrutins de niveau 2 et dans les 24 derniers mois pour les scrutins de niveau 1	
R-53	Le système de vote doit gérer le déroulement des différents scrutins de façon à pouvoir stopper totalement un scrutin sans que cela ait un impact sur les autres scrutins en cours. Le cloisonnement entre les scrutins peut être applicatif ou logique ou (optionnellement) physique, en fonction des besoins de l'organisateur.	0
R-55	Il est recommandé que le prestataire suive les bonnes pratiques de durcissement des systèmes, telles que les Recommandations de configuration d'un système GNU/LI NUX [Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022]. Il est recommandé que le prestataire suive les bonnes pratiques de durcissement des composants techniques du système de vote identifiés par la cartographie, telles que les recommandations des éditeurs des briques applicatives, celles issues de la liste National Checklist Program for IT Product [https://ncp.nist.gov/repository] ou celles émises par le Center for Internet Security [Center For Internet Security Benchmarks. https://www.cisecurity.org/cis-benchmarks-overview]	0
R-56	Il est recommandé que le prestataire et l'organisateur du scrutin suivent les bonnes pratiques pour l'administration du système de vote, telles que les Recommandations relatives à l'administration sécurisée des systèmes d'information [Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021]. En cas d'administration partagée entre l'organisateur du scrutin et le prestataire pour assurer les opérations de gestion et de maintenance, les accès au système de vote doivent suivre la même politique de sécurité, notamment concernant la journalisation des événements et les alertes.	0
R-57	Il est recommandé que le prestataire et l'organisateur du scrutin suivent les bonnes pratiques pour assurer la sécurité physique des composants techniques du système de vote, telles que les Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection [Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020].	0
	Mesures liées à l'authentification et la gestion des électeurs	
R-09	Le titulaire doit s'assurer, qu'en cas de recours à une solution d'authentification externe, indépendante du scrutin, cette solution présente les garanties suivantes : • Chaque électeur peut être authentifié. • S'il faut utiliser plusieurs solutions différentes pour couvrir l'ensemble des électeurs, il faut toutes les intégrer au système de vote. • Elle est accessible sur l'ensemble des équipements depuis lesquels les électeurs sont autorisés à voter. En particulier, si le recours à un équipement personnel est autorisé, alors la solution doit être exposée et utilisable depuis Internet. • La réglementation et les conditions générales d'utilisation de la solution pe mettent son utilisation dans le contexte du scrutin. • La solution renvoie une identité pivot qui peut être mise en relation de façon univoque avec la liste des électeurs du système de vote. • L'engagement de disponibilité de la solution est compatible avec les besoins du scrutin	0
R-10	À défaut d'une solution d'authentification existante adaptée, le système de vote doit utiliser un facteur de connaissance, tel qu'un mot de passe, dédié au scrutin, pour authentifier les électeurs.	0

N°	Exigence	Priorité
R-60	Pour renforcer l'authentification des électeurs, le système de vote doit combiner deux secrets d'authentification, dont un dédié au scrutin. Les cas suivants sont possibles : • Utiliser une solution d'authentification externe combinée avec un secret d'authentification dédié au scrutin. • Utiliser deux secrets d'authentification dédiés au scrutin, transmis par deux canaux différents.	0
R-11	Le système de vote doit mettre en œuvre des mécanismes d'authentification des électeurs conformes aux recommandations du guide Authentification multifacteurs et mots de passe [Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021]. Notamment : • Les secrets d'authentification doivent être générés avec suffisamment d'entropie. • Les secrets d'authentification doivent être générés au sein d'un environnement maîtrisé afin de prévenir tout accès illégitime à ces secrets. • Les fichiers contenant ces secrets doivent être protégés en confidentialité et en intégrité. • Les secrets d'authentification doivent être envoyés aux électeurs en garantissant leur confidentialité et leur intégrité (ils ne doivent notamment pas être envoyés en clair). • Le système de vote doit vérifier l'authentification des électeurs au moyen de données dérivées à partir des secrets d'authentification, et non directement au moyen de ces secrets. • Le système de vote doit être protégé contre les attaques par recherche d'authentifiants (attaques par force brute, par arrosage de mots de passe ou password spraying, par saisie d'authentifiants volés ou credential stuffing [2]). Ce type de protection peut s'appuyer sur un délai d'attente incompressible et croissant après plusieurs présentations de mots de passe erronés ou sur un CAPTCHA. • Le système de vote doit imposer une déconnexion automatique de l'électeur après un certain délai d'inactivité. L'électeur doit être informé de la déconnexion.	0
R-12	Lorsque le système de vote transmet des secrets d'authentification à des sous-traitants pour leur envoi aux électeurs (postal, par messagerie électronique, par SMS ou par messagerie instantanée), cette transmission doit assurer la confidentialité et l'intégrité des secrets. Une fois les secrets d'authentification des électeurs transmis au sous-traitant, celui-ci doit les protéger en confidentialité et en intégrité jusqu'à leur envoi aux électeurs. Le sous-traitant ne doit pas communiquer ces secrets à d'autres entités. Une fois les secrets envoyés, le sous-traitant doit supprimer toute copie de ces secrets (le sous-traitant n'a pas à conserver les secrets pour un éventuel recouvrement).	0
R-13	En cas d'envoi par courrier postal ou de remise en main propre d'un moyen d'authentification, il est recommandé que le système de vote assure la confidentialité de ce moyen en empêchant la lecture du secret sans ouverture de l'enveloppe.	0
R-14	Lorsque le système de vote met en place un recouvrement des secrets d'authentification, celui-ci ne doit pas abaisser la sécurité de l'envoi initial de ces secrets. Par défaut, les canaux utilisés pour l'envoi initial des secrets doivent être réutilisés pour le recouvrement. Le système de vote doit notifier l'électeur du recouvrement de son secret d'authentification par tous les canaux disponibles n'ayant pas servi au recouvrement. Cette notification permet à l'électeur d'être informé d'une demande de recouvrement illégitime faite en son nom. Le système de vote doit rendre inutilisables les secrets d'authentification précédents.	0

N°	Exigence	Priorité
R-15	Si l'organisateur du scrutin veut favoriser la participation en autorisant la saisie d'un nouveau moyen d'adressage (nouvelle adresse de messagerie, nouveau numéro de téléphone…) pour le recouvrement d'un secret d'authentification : • Il est recommandé que le système de vote authentifie l'électeur de façon renforcée, par exemple en utilisant une authentification externe (système d'authentification de l'entité à laquelle appartiennent les électeurs, identité numérique, vérification d'identité à distance [Prestataires de vérification d'identité à distance (PVID). https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid]) ou grâce à un défi-réponse conforme au guide Authentification multifacteurs et mots de passe [Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021]. • Si l'authentification renforcée réussit, si le défi réussit ou encore si l'absence d'authentification renforcée ou de défi-réponse est jugée acceptable par l'organisateur du scrutin, le système de vote permet à l'électeur de saisir un nouveau moyen d'adressage. • Le système de vote électronique renouvelle le secret et l'envoie vers le nouveau moyen d'adressage.	0
	Mesures liées à la cryptographie et au secret du vote	
R-03	Le système de vote doit mettre en œuvre des mécanismes cryptographiques conformes aux *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [Guide ANSSI-PG-083 v3.0, ANSSI, mars 2026]	0
R-16	Le système de vote doit présenter aux électeurs un client de vote assurant la confidentialité du suffrage, notamment : • Le client de vote doit réaliser le chiffrement du suffrage au moyen de mécanismes cryptographiques implémentés conformément au *Guide de sélection d'algorithmes cryptographiques* [Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.]. En particulier, lorsque le client de vote fait appel à des bibliothèques cryptographiques (par exemple du navigateur), ces bibliothèques doivent être éprouvées et les appels à ces bibliothèques doivent être réalisés conformément aux préconisations des fournisseurs de ces bibliothèques. • Le client de vote ne doit pas faire appel à des ressources tierces en ligne non maîtrisées. • Le client de vote doit maîtriser l'accès aux données sensibles (suffrage, aléa utilisé pour le chiffrement du suffrage) au sein et en dehors du navigateur, puis assurer leur effacement dès que le bulletin est créé	0
R-18	Le client de vote doit effectuer le chiffrement du suffrage de l'électeur au moyen d'un mécanisme de chiffrement asymétrique probabiliste non-malléable, dès que l'électeur a validé son suffrage. Dans ce cas, le client de vote doit être en mesure de générer suffisamment d'aléa localement et de le combiner si nécessaire avec une source d'aléa externe maîtrisée (par exemple en provenance du serveur de vote).	0
R-19	Il est recommandé que le prestataire analyse la conformité du mécanisme de chiffrement des suffrages avec les mécanismes cryptographiques suivants : • L'accumulation des bulletins. • Le mélange cryptographique (et le mélange vérifiable) des bulletins. • Le partage de secret à seuil. • Le déchiffrement vérifiable. Il est recommandé que cette analyse s'appuie sur des travaux académiques de référence, c'est-à-dire publiés à des conférences ou dans des journaux scientifiques reconnus en cryptographie ou en sécurité informatique.	0
R-20	En cas de pastillage, le système de vote doit associer les attributs de l'électeur au bulletin chiffré. De plus :	0

N°	Exigence	Priorité
	• La mise en œuvre du pastillage ne doit pas porter atteinte au secret du scrutin. • L'électeur doit être informé sur les scrutins indirects auxquels il participe et des moyens lui permettant de vérifier la prise en compte de son suffrage pour tous ces scrutins. • La mise en œuvre du pastillage doit permettre de détecter tout déplacement d'un bulletin d'une urne à l'autre.	
R-28	Il est recommandé que le système de vote ne réalise pas d'horodatage individuel des bulletins transmis par les électeurs, c'est-à-dire qu'il ne produise pas de trace horodatée contenant soit le bulletin, soit une information calculée de manière déterministe à partir du bulletin (par exemple une empreinte du bulletin). Cela implique en particulier que les journaux d'événements établis aux fins de surveillance du système de vote ne contiennent pas de bulletin ni aucune information calculée de manière déterministe à partir du bulletin.	0
R29	Le système de vote doit assurer l'étanchéité entre l'identité de l'électeur et l'expression de son vote par accumulation ou mélange cryptographique des bulletins. Dans les deux cas, le mécanisme mis en œuvre doit être compatible avec le mécanisme de chiffrement des suffrages. La solution de vote doit assurer que seuls les bulletins accumulés ou mélangés, sont déchiffrés : • En cas d'accumulation, l'accumulation ne peut être réalisée qu'après vérification individuelle de la validité des suffrages (sans divulgation de ceux-ci) contenus dans les bulletins et le déchiffrement ne peut être réalisé que sur l'accumulation produite et pas sur les bulletins d'origine. • En cas de mélange cryptographique incluant le déchiffrement, le mélange ne peut être réalisé qu'après vérification individuelle de la validité des bulletins. • En cas de mélange cryptographique n'incluant pas de déchiffrement, le mélange ne peut être réalisé qu'après vérification individuelle de la validité des bulletins, et le déchiffrement ne peut être réalisé que sur les bulletins issus du mélange.	0
R-30	Le système de vote doit assurer la propriété de receipt-freeness : l'ensemble des données transmises ou affichées par le système de vote ne doivent pas permettre à l'électeur de prouver son suffrage à un attaquant, également destinataire de ces données.	0
R-31	Le système de vote doit fragmenter la clé privée de déchiffrement des bulletins au moyen d'un mécanisme de partage de secret à seuil, compatible avec le mécanisme de chiffrement des suffrages. Le partage doit être effectif (il y a strictement plus de deux fragments) et le seuil doit être effectif (il doit être strictement plus grand que 1). Le déchiffrement ne doit être possible qu'avec un nombre de fragments supérieur ou égal au seuil, y compris lorsque ce déchiffrement intervient afin d'exécuter un nouveau décompte. La description de la fragmentation (les porteurs de fragments, le seuil utilisé) doit être publique.	0
R32	Le système de vote doit stocker les fragments de la clé privée de l'élection en respectant les points suivants : • La clé privée entière (non fragmentée) ne doit jamais être stockée. • À chaque fragment de la clé privée doit être associé un code d'activation, seulement connu de l'attributaire. • Le système de vote doit imposer une règle de composition du code d'activation afin de le rendre conforme aux Recommandations relatives à l'authentification multifacteur et aux mots de passe [Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021]. Cette règle doit tenir compte de l'utilisation du code dans la protection du fragment de clé privée (code permettant de déri	0

N°	Exigence	Priorité
	ver une clé symétrique de chiffrement ou bien code PIN d'activation de support matériel). • Chaque fragment de la clé privée est enregistré individuellement en étant chiffré. Cet enregistrement peut être réalisé dans le système de vote électronique, ou sur un support physique qui est alors remis à l'attributaire du fragment. • L'enregistrement protège le fragment en intégrité et en confidentialité et le fragment ne peut être déchiffré et utilisé qu'en connaissant le code d'activation. • Les codes d'activation ne sont pas enregistrés par le système de vote électronique. • Les codes d'activation ne doivent pas être rassemblés sous le contrôle d'un nombre plus réduit d'acteurs (organisateur ou prestataire) que le seuil. Note : *Une pratique répandue consiste à organiser une cérémonie au cours de laquelle les fragments de la clé privée de l'élection sont générés et chaque attributaire choisit un code d'activation. Cette cérémonie permet de réunir le bureau électoral et de réaliser d'autres actions comme la mise en œuvre de scellements.*	
	Mesures liées aux opérations de vote et transport	
R-07	Dès lors que l'électeur a exprimé et validé son choix, le système de vote doit enchaîner l'ensemble des traitements constituant l'opération de vote sans discontinuité jusqu'à l'achèvement du dernier traitement, la délivrance d'un récépissé. L'échec d'un traitement entraîne l'échec de toute l'opération et, a contrario, la réussite de l'opération n'est possible que de par le succès de chacun des traitements unitaires. Les traitements les plus critiques sont le dépôt du bulletin dans l'urne et l'émargement, qui doivent être réalisés de manière indissociable afin d'assurer leur cohérence.	0
R-08	Le système de vote doit délivrer un récépissé à l'électeur à la fin de l'opération de vote. Il est acceptable que le récépissé soit généré dans le cadre de l'opération de vote, puis délivré de façon asynchrone par messagerie électronique. Le récépissé doit contenir les informations requises par la réglementation encadrant le scrutin (suivant les cas, un identifiant de l'électeur, l'horodatage de l'opération de vote ainsi que le ou les scrutins auxquels l'électeur a participé). Le récépissé ne doit pas contenir d'informations liées au bulletin de l'électeur, informations présentes dans la preuve de vote.	0
R-17	Lorsque le client de vote est un JavaScript intégré à la page Web présentée à l'électeur et exécuté par son navigateur, il est recommandé que le système de vote intègre des mécanismes de détection des caractéristiques techniques de l'équipement utilisé par l'électeur pour réaliser son vote (version de navigateur, moteur JavaScript, activation de la sandbox, mode debug). Ces détections doivent permettre au client de vote : • D'empêcher son exécution sur un navigateur ou un moteur JavaScript incompatibles car n'ayant pas les caractéristiques requises. Par exemple, le client de vote ne devrait pas s'exécuter sur une version de navigateur ayant une CVE connue permettant la fuite de données ou n'implémentant pas une version de TLS compatible. • De lier son exécution à l'activation de mécanismes d'isolation afin de restreindre la modification ou la récupération illégitime de données. • D'empêcher son exécution lorsque le mode debug du moteur JavaScript ou du navigateur est activé, afin de restreindre la modification ou la récupération illégitime de données.	0
R-21	Le prestataire doit décrire précisément le chemin complet du bulletin de vote du client de vote jusqu'à l'urne électronique.	0

N°	Exigence	Priorité
	Cette description doit contenir l'ensemble des composants du système de vote par lesquels transitent les bulletins une fois qu'ils sont traités par la terminaison TLS exposée aux électeurs, jusqu'à l'urne électronique, notamment en cas de mise en œuvre d'une architecture « trois tiers ». Le prestataire doit identifier clairement les terminaisons TLS et les points de rupture du protocole sur ce chemin.	
R-22	Le système de vote doit mettre en place des liaisons TLS conformes aux Recommandations de sécurité relatives à TLS [Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020] pour l'ensemble des flux initiés par le client de vote. Le client de vote doit authentifier le serveur de vote grâce à un certificat (authentification simple). La négociation des liaisons TLS doit être paramétrée de façon stricte et exclure les versions de TLS et les mécanismes cryptographiques obsolètes. Le système de vote doit mettre en place un certificat conforme aux préconisations du Référentiel Général de Sécurité [Référentiel Version 2.0, ANSSI, juin 2012. https://cyber.gouv.fr/rgs]	0
R-23	Il est recommandé que le système de vote mette en place des liaisons TLS à double authentification (comportant l'authentification du serveur et l'authentification du client) conformes aux Recommandations de sécurité relatives à TLS [Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020] pour l'ensemble des flux sur le chemin entre la terminaison TLS exposée aux clients de vote et l'urne électronique.	0
R-24	Il est recommandé que le système de vote mette en œuvre un mécanisme de vérification de la validité des bulletins transmis par les électeurs ainsi qu'un mécanisme de vérification du suffrage contenu dans le bulletin, sans divulguer le suffrage ni l'aléa utilisé pour le chiffrement. Dans ce cas, le serveur de vote doit vérifier cette validité à la réception du bulletin et le rejeter si la vérification échoue. En cas d'accumulation des bulletins pour assurer l'étanchéité bulletin/suffrage, un mécanisme attestant de la validité du suffrage sans le divulguer est obligatoire.	0
R-27	Le système de vote doit permettre de détecter toute perte ou modification illégitime des bulletins transmis par les électeurs, traités par le serveur de vote et stockés dans l'urne électronique, jusqu'au dépouillement. Il est recommandé d'utiliser une signature numérique ou un chaînage des bulletins : une telle modification est détectable, car elle rend la signature ou le chaînage invalide	0
R-33	La solution de vote doit détecter (de façon organisationnelle ou technique) toute tentative de réaliser le dépouillement avant la clôture du scrutin et toute tentative de réaliser le dépouillement sur d'autres ensembles de bulletins que ceux prévus par l'élection. En cas de pastillage, les urnes électroniques à dépouiller sont celle du scrutin direct et celles des scrutins indirects.	0
	Mesures liées à l'intégrité du système et scellement	
R-34	Il est recommandé que le prestataire fournisse une compilation reproductible du code source de l'application de vote en fichiers exécutables déployés sur le système de vote. La compilation de l'application de vote doit pouvoir être reproduite de manière indépendante par un tiers (par exemple l'expert indépendant au sens de la délibération de la CNIL) et générer les mêmes fichiers exécutables que dans l'environnement de compilation du prestataire. Le résultat de la compilation reproductible peut être identifié par une prise d'empreinte numérique.	0
R-35	Le système de vote doit permettre à un expert indépendant (au sens de la délibération de la CNIL [Délibération n° 2026-045 du 19 mars 2026 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance	0

N°	Exigence	Priorité
	électronique et abrogeant les délibérations n° 2010-371 du 21 octobre 2010 et n° 2019-053 du 25 avril 2019]) de contrôler que les fichiers exécutables de l'application de vote correspondent au résultat de la compilation du code source objet de l'expertise. L'intégrité de ces fichiers exécutables doit pouvoir être vérifiée par un calcul d'empreinte numérique et une comparaison avec l'empreinte de référence, issue de la compilation reproductible. De plus, l'application de vote peut inclure des scripts ou des fichiers non exécutables (par exemple, le schéma de la base de données) dont l'intégrité doit pouvoir être vérifiée, également par comparaison d'empreinte numérique.	
R-36	Le système de vote doit permettre au prestataire de contrôler la cohérence de l'urne électronique et de la liste d'émargement tout au long du scrutin. Elles doivent être vides à l'ouverture du scrutin, elles ne doivent qu'augmenter pendant le scrutin et elles doivent comporter à tout moment le même nombre d'éléments. En cas de pas tillage, la cohérence doit être vérifiée sur l'urne du scrutin direct et les urnes des scrutins indirects. La cohérence doit pouvoir être contrôlée par requêtes directes, qui doivent donner le nombre exact d'entrées dans l'urne et dans la liste d'émargement de chaque scrutin.	0

R-45	Le système de vote doit mettre en œuvre des scellements, par exemple en suivant les Recommandations de configuration d'un système GNU/LINUX [Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022] : une opération de scellement d'un système de fichiers peut consister en l'installation puis la configuration d'un service qui aura pour objectif de vérifier périodiquement les modifications faites au niveau d'une arborescence.
	
	Dans ce cas, les scellements doivent être conformes aux Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques [18] et notamment porter sur les éléments suivants :
	• Avant l'ouverture du scrutin :
	  ○ Les données relatives à l'application de vote.
	  ○ Les données relatives à la configuration de l'élection. La configuration inclut notamment le découpage électoral, les options de vote et l'ordre dans lequel elles sont présentées aux électeurs, la liste électorale, les heures d'ouverture et de fermeture du scrutin, la clé publique de l'élection et les éventuels secrets de signature numérique (en particulier des preuves de vote quand elles sont mises en œuvre), de chaînage ainsi que le pastillage.
	• À la clôture du scrutin : sur l'urne électronique et la liste d'émargement.
	• À la fin du dépouillement sur l'ensemble des données générées (fichiers de résultats, procès-verbaux, preuves générées par le système de vote, le cas échéant).
		0

R-46	Le système de vote doit vérifier périodiquement les scellements mis en œuvre. Dans ce cas, le déclenchement de cette vérification doit être aléatoire afin de rendre les contrôles non prévisibles. La fréquence des contrôles doit dissuader une tentative d'intervention non autorisée sur le système de vote et doit assurer une détection rapide de toute altération.	0
	Mesures liées à la disponibilité et l'infrastructure	
R-25	Il est recommandé que le système de vote fournisse une PDMA (perte de données maximale admissible) nulle : aucun bulletin ne doit être perdu pendant le scrutin.	0
R-26	Le prestataire doit restreindre ses accès techniques au système de vote pendant le scrutin aux opérations de gestion et de maintenance strictement nécessaires au maintien en condition opérationnelle et en condition de sécurité du système de vote.	0

N°	Exigence	Priorité
R-41	Le système de vote doit être correctement dimensionné pour supporter l'élection et la charge attendue. Cela concerne l'ensemble du système de vote, tel qu'il a été cartographié (R4‹). L'organisateur du scrutin doit fournir au prestataire les éléments lui permettant de réaliser ce dimensionnement, notamment : • Le nombre d'électeurs a un impact sur la charge du système de vote avant et pendant le vote, et sur le volume des échanges, des données produites et des traces générées par le système de vote. • Le nombre d'options de vote (ex. : candidats) et le pastillage ont un impact sur les traitements réalisés par le client de vote. • Le nombre d'électeurs et le nombre d'options de vote ont un impact sur les traitements nécessaires pour réceptionner, traiter, accumuler ou mélanger, et déchiffrer les bulletins. Si des ressources sont partagées entre le système de vote et d'autres systèmes (serveurs, stockage, réseau), le prestataire doit s'assurer des ressources nécessaires au fonctionnement du système de vote, indépendamment du fonctionnement des autres systèmes	0
R-42	Le prestataire doit fournir un système secondaire susceptible de prendre le relais en cas d'incident sur le système principal, et offrant les mêmes garanties et les mêmes caractéristiques. De plus, il est recommandé que chaque système (principal ou secondaire) s'appuie sur une redondance d'infrastructure technique.	0
R-43	Il est recommandé que le prestataire effectue une supervision technique de l'état du système de vote, notamment des éléments suivants : l'état des serveurs et des équipements réseau (utilisation du CPU et de la RAM), l'état des disques (volume occupé), l'état du réseau (volume des données échangées) et l'état des services (serveurs Web et applicatifs, serveur de base de données...). Dans ce cas, le prestataire doit avoir accès à ces informations en temps réel pour contrôler le fonctionnement correct du système de vote.	0
R-44	Il est recommandé que le système de vote soit protégé contre les attaques par déni de service afin de limiter leur impact pendant la période de vote, par exemple en appliquant les *Essentiels de l'ANSSI- Dénis de service distribués* [Essentiels Version 2.0, ANSSI, avril 2024. https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos] ainsi que les *Fiches Réflexes du CERT-FR* [Fiche réflexe du CERT-FR. Déni de service réseau- Endiguement. https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-010/, Fiche réflexe du CERT-FR. Déni de service réseau- Qualification. https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-009/].	0
R-47	Il est recommandé que le prestataire effectue une supervision technique des accès au système de vote, notamment les accès distants aux serveurs, au système de gestion des bases de données et aux équipements réseau.	0
	Mesures liées à la journalisation au contrôle et aux alertes	
R-37	Il est recommandé que le prestataire mette en œuvre un système de journalisation des événements, par exemple en suivant les *Recommandations de sécurité pour l'architecture d'un système de journalisation* [Guide DAT-PA-012 v2.0, ANSSI, janvier 2022]. Dans ce cas, les événements journalisés ne doivent pas contenir les données suivantes : • Les secrets d'authentification des électeurs. • Les secrets ou clés privées de signature numérique ou de chaînage des bulletins. • Les fragments de la clé privée de l'élection et les codes d'activation des attributaires. • Les secrets ou clés privées utilisés pour le scellement du système de vote.	0

N°	Exigence	Priorité
	• Les bulletins des électeurs ou toute information calculée de manière déterministe à partir des bulletins (par exemple une empreinte numérique des bulletins). • Les informations présentes dans les preuves de vote. De plus, il est recommandé que le prestataire soit en mesure d'analyser les journaux *en temps réel* pour contrôler le fonctionnement correct du système de vote et *a posteriori* pour analyser les causes d'un éventuel dysfonctionnement.	
R-38	Il est recommandé que le système de vote journalise les événements relatifs à son fonctionnement, notamment : • Toute opération de maintenance et de gestion réalisée sur le système de vote. • Le déploiement de la configuration de l'élection et des fichiers exécutables. • La génération des secrets d'authentification des électeurs. • L'envoi (dont l'envoi initial s'il est réalisé par le système de vote) et le recouvrement des secrets d'authentification des électeurs; le changement de moyen d'adressage des secrets d'authentification des électeurs. • La génération des clés privées ou des secrets de signature numérique ou de chaînage et de la clé privée de signature numérique des preuves de vote. • La génération des fragments de la clé privée de l'élection. • L'ouverture, la suspension, l'arrêt et la fermeture du scrutin. • Les traces générées par le chaînage. • La réalisation du dépouillement, y compris le lancement et la clôture des opérations d'accumulation, de mélange cryptographique et de déchiffrement. • Le scellement et toute vérification de scellement du système. • Les alertes transmises au bureau électoral.	0
R-39	Il est recommandé que le système de vote journalise les événements ayant un impact direct ou indirect sur le secret du scrutin, l'intégrité des suffrages exprimés et la sincérité des opérations électorales, notamment : • Accès illégitime à la clé privée de l'élection ou un de ses fragments. • Échec d'un traitement de l'opération de vote. • Dépôt d'un bulletin dans une urne électronique sans émargement ou émargement sans dépôt de bulletin dans une urne électronique. • Attaque par recherche d'authentifiant. • Détection de modification de bulletin transmis par un électeur, traité par le serveur de vote et stocké dans l'urne électronique. • Indisponibilité du système de vote. • Attaque en déni de service sur le système de vote. • Rupture d'un scellement.	0
R-48	Le prestataire doit fournir au bureau électoral les résultats des différents contrôles d'intégrité mis en œuvre par le système de vote : • Contrôle de l'intégrité de l'application de vote. • Contrôle de cohérence entre l'urne et la liste d'émargement décrit. • Contrôle des scellements.	0
R-49	Le prestataire doit permettre à un tiers d'analyser les journaux collectés pendant les opérations, contenant les événements relatifs au fonctionnement du système de vote ainsi que les événements ayant un impact sur la sincérité du scrutin. Le prestataire doit s'assurer que les libellés des événements sont suffisamment compréhensibles pour que le tiers puisse en réaliser l'analyse en toute autonomie. Le	0
R-50	Le prestataire doit permettre au bureau électoral de déclencher manuellement et en autonomie (sans intervention du prestataire ni de l'organisateur du scrutin) les contrôles d'intégrité : • Contrôle de l'intégrité de l'application de vote. • Contrôle de cohérence entre l'urne électronique et la liste d'émargement.	

N°	Exigence	Priorité
	• Contrôle des scellements. Les contrôles manuels doivent pouvoir être déclenchés pendant toute la période de vote.	
R-51	Le système de vote doit émettre des alertes à destination du bureau électoral pour tout événement ou incident relatif à la sécurité du système de vote, ayant un impact sur le secret du scrutin, la sincérité des opérations électorales, l'intégrité des suffrages exprimés, l'accès au vote pour tous les électeurs Ces alertes doivent être générées et être transmises automatiquement et sans délai par le système de vote, sans que le prestataire n'ait à intervenir pour qu'elles par viennent au bureau électoral. Toute modification du système d'alerte doit également générer une alerte automatique au bureau électoral.	0
R-52	Le prestataire doit mettre en œuvre un système d'alerte à destination du bureau électoral, l'informant de toute intervention de gestion et de maintenance sur le système de vote. Ces alertes doivent être générées et être transmises automatiquement par le système de vote, sans que le prestataire n'ait à intervenir pour qu'elles parviennent au bureau électoral. Toute modification du système d'alerte doit également générer une alerte automatique vers le bureau électoral.	0
	Mesures liées à la vérifiabilité, la transparence et le dépouillement	
R-40	En l'absence de déchiffrement vérifiable ou en cas de contrainte réglementaire, le système de vote doit permettre la vérification du dépouillement par l'exécution d'un nouveau décompte. Cette vérification part de l'urne électronique d'origine et exécute à nouveau, le cas échéant l'accumulation ou le mélange cryptographique, et le déchiffrement. Dans ce cas, la procédure de conservation des fragments de la clé privée de l'élection et des codes d'activation associés doit assurer le secret du scrutin.	0
R-58	Le client de vote doit générer une preuve de vote, permettant à l'électeur de vérifier la présence de son bulletin dans l'urne. L'électeur peut conserver la preuve de vote. La preuve de vote contient une référence cryptographiquement liée au bulletin (par exemple une empreinte numérique du bulletin ou bien une preuve à divulgation nulle de connaissance), calculée au moment où le votant valide son suffrage. La preuve de vote ne doit pas contenir l'identité de l'électeur ni l'horodatage de son vote. La preuve de vote ne doit pas non plus contenir de données qui, seules ou ajoutées aux informations fournies par le récépissé de vote, portent atteinte au secret du scrutin ou facilitent l'achat de vote. La référence est transmise au serveur de vote pour publication. Il est recommandé que la preuve de vote contienne également une signature de cette référence par le serveur de vote.	0
R-59	Le serveur de vote doit rendre publique une liste des références présentes dans les preuves de vote transmises par les clients de vote sur une page Web accessible sans restriction depuis Internet. Le serveur de vote doit également rendre publique la clé publique de vérification de la signature des références dans les preuves de vote, également sur une page Web accessible sans restriction depuis Internet. Pendant le scrutin et jusqu'à expiration des délais de recours, les électeurs doivent disposer d'un moyen pour contrôler que la référence présente dans leur preuve de vote et correspondant à leur bulletin est bien présente dans la liste des références rendue publiquement disponible par le système de vote et que sa signature est correcte	0

N°	Exigence	Priorité
R-61	En amont du scrutin, le prestataire doit rendre public le protocole de vote qu'il met en œuvre dans le système de vote sans préjudice de la propriété intellectuelle du prestataire. Cette publication peut typiquement s'effectuer sur une page Web accessible sans restriction depuis Internet. Cette publication doit notamment comprendre : • Les messages échangés entre tous les acteurs, l'ordre dans lequel ces messages sont échangés, les traitements effectués à chaque étape par chaque acteur (notamment la récupération ou le stockage de données intermédiaires, l'affichage ou la demande d'information à l'utilisateur, la vérification de signature numérique, les preuves à divulgation nulle de connaissance, les tests d'égalité). La description doit être aussi précise que possible pour chaque acteur. • Les éventuelles références académiques sur lesquelles s'appuie le protocole utilisé, ainsi que les éventuels écarts avec ces références. • Les mécanismes cryptographiques mis en œuvre pour assurer la confidentialité et l'intégrité des données tout au long du scrutin. • Les propriétés de sécurité prétendument atteintes, leur modèle de confiance et un argumentaire décrivant comment ces propriétés sont atteintes. • Les composants et acteurs intervenant dans l'élection (notamment client de vote, serveur de vote, électeur, bureau électoral). • La description des cérémonies, notamment celles faisant intervenir le bureau électoral. La description des échanges doit permettre à un tiers de contrôler que les propriétés de sécurité prétendument atteintes le sont réellement. Cette analyse de sécurité doit être autorisée pour tout tiers (et pas seulement l'expert indépendant au sens de la délibération de la CNIL), sur la base des spécifications publiées. Un point de contact doit être identifié pour rendre possible la divulgation responsable d'éventuelles faiblesses identifiées par les tiers.	0

Responsabilité

Référence	Libellé exigence	Priorité
SECU_001	L'organisation de la sécurité des systèmes d'information du titulaire pour le projet est décrite dans le PAS. L'équipe comporte a minima : ▪ Une personne de niveau hiérarchique supérieur formé et compétent en SSI capable de prendre des décisions dans la conduite du projet, responsable du respect des dispositions du PAS ▪ Une personne intégrée ou proche des équipes de MOE du titulaire en charge du projet responsable de la mise en œuvre du PAS ▪ La rédaction, la mise à jour et le suivi du PAS sont à la charge du titulaire	0

Dans l'exercice de leurs activités, les intervenants sont liés par un devoir de réserve et astreints au secret professionnel.

Sensibilisation, qualification et formation

Référence	Libellé exigence	Priorité
SECU_002	Le titulaire indique au CNRS la fréquence et le contenu des actions de formation et de sensibilisation de ses personnels aux enjeux et aux méthodes de Sécurité.	0

5.6.2 Protection des biens

Protection des sites

Référence	Libellé exigence	Priorité
SECU_003	Si le titulaire exécute les prestations à partir de ses propres locaux, il opère en « *site sûr* » dont les caractéristiques sont à évaluer avec le département Sécurité de la DSI. Cette	1

Référence	Libellé exigence	Priorité
	disposition est également valable pour le support ou la maintenance à distance. Le titulaire ne détient à aucun moment de données de production signifiantes sur ses infrastructures. Le cas échéant, le titulaire réalise un dossier de type « *site sûr* » incluant les modalités d'accès aux ressources de la DSI et les mesures de sécurité nécessaires à l'accomplissement des prestations. Si un Plan d'Assurance Sécurité existe, le dossier « *site sûr* » lui sera annexé.	
SECU_004	Le titulaire fournit un dossier de site sûr décrivant les mesures de sécurité physique en place dans les locaux qu'il utilise pour l'accomplissement des prestations. Ce dossier traite des thématiques suivantes sous les angles **technique** et **organisationnel** : ▪ Infrastructures informatiques (réseaux et systèmes) ▪ Contrôle d'accès physique aux locaux ▪ Contrôle d'accès logique aux systèmes ▪ Postes de travail ▪ Liaisons réseaux externes (WAN, réseaux privés avec le CNRS) ▪ Plan de reprise/de continuité d'activité ▪ Gestion de crise	0

Protection du système d'information

Référence	Libellé exigence	Priorité
SECU_005	Le titulaire dispose de dispositifs, de procédures et de moyens qu'il met en œuvre afin protéger les actifs du CNRS. Ces moyens permettent en particulier de : ▪ contrer les virus et codes malveillants ▪ protéger son réseau contre les intrusions. Il décrit les mesures mises en œuvre.	0

Politique de contrôle d'accès

Référence	Libellé exigence	Priorité
SECU_006	Le titulaire dispose d'une politique, de mesures et de dispositifs pour gérer le contrôle d'accès à ses locaux et à ses systèmes d'information. Cette politique concerne notamment : ▪ la politique d'attributions des droits ▪ les méthodes d'accès (authentification et autorisation) ▪ la gestion des identifiants uniques ▪ la politique de mots de passe et de gestion de l'authentification forte ▪ les processus d'autorisation pour l'accès et les privilèges des utilisateurs ▪ les processus de gestion des listes de personnes autorisées à participer aux activités de TMA ▪ les processus de révocation des droits ▪ la politique et les processus de révision des droits d'accès ▪ le contenu de la charte interne utilisateur et/ou de la charte interne administrateur Le titulaire décrit les mesures en place. Il fournit en particulier sa PSSI d'entreprise.	0

Gestion des vulnérabilités

Référence	Libellé exigence	Priorité
SECU_007	Le titulaire dispose de procédures de gestion interne des vulnérabilités sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support. Il décrit les méthodes et outils en place pour la découverte et le suivi de la correction de ces vulnérabilités.	0

Gestion des incidents

Référence	Libellé exigence	Priorité
SECU_008	Le titulaire dispose de procédures de gestion des incidents internes de sécurité sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support.	0

Exigences de Sécurité concernant les personnels extérieurs

Référence	Libellé exigence	Priorité
SECU_009	Le titulaire met en œuvre des moyens de contrôle pour s'assurer du respect des exigences de sécurité du CNRS par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre des prestations. Il fournit les éléments contractuels le liant avec ses partenaires prouvant les obligations qui leur incombent dans ce domaine.	0

Travail dans les zones sécurisées

Référence	Libellé exigence	Priorité
SECU_010	Le titulaire ne doit jamais intervenir physiquement sur un site du CNRS ou géré par le CNRS sans être mandaté et surveillé par du personnel du CNRS ou mandaté par le CNRS. Il doit refuser d'assurer sa prestation, si le personnel encadrant du CNRS ou mandaté par le CNRS ne respecte pas son obligation de surveillance. Il notifie l'incident à sa direction et au RSSI de la DSI. Le délai d'exécution de la prestation est suspendu jusqu'à ce que le personnel encadrant du CNRS ait pris les mesures nécessaires à cette surveillance. Le titulaire n'est pas autorisé, sauf autorisation expresse du CNRS, à photographier, faire des enregistrements audio ou vidéo des locaux ou des équipements du CNRS. De même, il est interdit au titulaire d'introduire du matériel photographique, vidéo, audio ou d'autres matériels d'enregistrement dans les locaux du CNRS ou géré par le CNRS, sauf autorisation expresse du CNRS.	0

Stockage et échange d'informations

Référence	Libellé exigence	Priorité
SECU_011	Le titulaire met en œuvre des moyens techniques conformes aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) afin de protéger de toutes divulgations indésirables volontaires ou accidentelles, toutes les informations relatives au CNRS : ▪ lors du stockage de celles-ci en dehors des sites physiques du CNRS, pendant et après les prestations. ▪ lors des échanges avec le CNRS, quel qu'en soit le moyen (e-mail, partage de fichier, etc.). De plus le titulaire effacera les informations qu'il aura en sa possession, immédiatement et en fournissant au CNRS un quitus formel : ▪ sur simple demande du CNRS ▪ en fin de prestation	0

Gestion des sauvegardes

Référence	Libellé exigence	Priorité
SECU_012	Le titulaire donne au CNRS l'ensemble des éléments techniques concourant à une sauvegarde intègre et régulière des données du CNRS qui lui sont confiées et des données nécessaires à l'exécution des prestations (plan de sauvegarde, procédures, script d'arrêt/démarrage, objets à sauvegarder, intégrité temporelle des données, etc.). La solution du titulaire doit permettre au CNRS de mettre en place des tests réguliers de restauration des sauvegardes.	0

Rétrocession des informations du CNRS

Référence	Libellé exigence	Priorité
SECU_013	Le titulaire précise les mesures et dispositifs qui garantissent le retour au CNRS et la destruction des informations du CNRS qu'il a en sa possession à l'expiration ou à la résiliation du marché. Le titulaire fournit au CNRS l'ensemble de la documentation nécessaire et une description précise des éléments techniques permettant au CNRS d'extraire les données de la solution dans un format compréhensible (*par exemple fichier csv et schéma relationnel des données*). Ces éléments doivent permettre au CNRS de reprendre ces données dans une autre solution le cas échéant.	0

5.6.3 Obligations du titulaire

Référence	Libellé exigence	Priorité
SECU_014	Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage à informer le CNRS des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Le titulaire est responsable du maintien en condition de sécurité des systèmes nécessaires à la réalisation des prestations jusqu'à leur échéance. Le titulaire ne peut se dégager de cette responsabilité que si, après qu'il ait informé le CNRS de failles dans la sécurité du système, de manière circonstanciée, précise et détaillée, et qu'il ait proposé une ou des solutions de nature à pallier la faille, le CNRS a choisi de ne pas mettre en œuvre ces préconisations.	0

5.6.4 Localisation des données

Référence	Libellé exigence	Priorité
SECU_015	Les lieux d'hébergement des données du CNRS, dont les journaux, les jeux d'essai pour les environnements de développement (liste non-exhaustive), satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la loi informatique et libertés en vigueur. Tout transfert de données en dehors des Etats de l'UE est soumis à avis, et autorisation préalable du CNRS, après avis de son Délégué à la Protection des Données. Le titulaire communique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Enfin, le titulaire doit fournir au CNRS tous les éléments attestant qu'il satisfait bien aux exigences réglementaires ci-dessus, quel que soit la localisation.	0

5.6.5 Audit

Référence	Libellé exigence	Priorité
SECU_016	Le titulaire est informé de la volonté du CNRS de conduire ou organiser des audits réguliers des systèmes d'information. Ces audits techniques et organisationnels ont pour objectifs de vérifier le respect par le titulaire de ses engagements initiaux en termes d'organisation et de moyens mis en œuvre concernant la SSI. Le CNRS peut, à tout moment, à son initiative, par ses propres équipes ou par celles de tiers désignés par lui (sélectionnés sur la liste des prestataires qualifiés en audit SSI publiée sur le site de l'ANSSI à la date de commande de l'audit https://messervices.cyber.gouv.fr/visas/catalogue-produits-services-profils-de-protection-sites-certifies-qualifies-agrees-anssi.pdf), procéder à des audits des prestations confiées au titulaire, afin de :	0

	▪ vérifier les engagements de niveaux de service, de qualité, de sécurité des prestations réalisées ; ▪ vérifier la mise en application des règles d'organisation, des méthodes, des pratiques mises en œuvre pour réaliser les prestations. À cet effet, le CNRS ou son mandataire désigné met en œuvre tous les moyens qu'il juge nécessaire pour s'assurer du parfait achèvement des prestations. Ceci inclut, sans volonté d'exhaustivité : ▪ la communication de documents tenus à jour par le titulaire (plans, documentations, contrats, certifications, rapports…) ; ▪ l'audition orale d'équipes de maîtrise d'œuvre (techniciens, ingénieurs, responsables techniques, opérationnels, responsables de la sécurité, équipes de direction…) ; ▪ la conduite de tout audit organisationnel ou technique, en boîte blanche, noire ou grise. Le CNRS s'engage à respecter un préavis raisonnable conforme aux dispositions du CCAP avant tout déclenchement d'audit. Le résultat des audits est présenté au titulaire, et conduit à la rédaction d'un plan d'action. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : ▪ à ses engagements initiaux ou ▪ à la réglementation en vigueur à la date de notification de l'appel d'offres. Dans tous les autres cas (évolution de la réglementation, évolution de la PSSI du CNRS, évolution d'une application modifiant son profil de risque...), le titulaire peut proposer une cotation pour la réalisation des prestations de mise en conformité. Le résultat des audits de conformité aboutit à un avis formel du CNRS ▪ conforme : l'audit n'a pas révélé de dysfonctionnements majeurs, et les engagements qui ont été audités sont tenus ; ▪ conforme avec réserves : des dysfonctionnements mineurs ont été relevés ou des objectifs ne sont pas remplis au niveau de l'engagement de service attendu. Dans ce cas, le titulaire propose un plan de remédiation aux dysfonctionnements à court terme : le plan est soumis au CNRS dans les huit jours après communication de l'avis formel, et l'engagement de remédiation ne peut dépasser six mois. Le titulaire démontre à ses frais que les engagements sont tenus à l'issue du plan d'action ; ▪ non conforme : tout ou partie des engagements ne sont pas tenus, ou des dysfonctionnements majeurs ont été constatés. Dans ce cas, le titulaire engage des actions selon les modalités décrites supra, sous astreinte journalière de remise en conformité.	

5.6.6 Application des plans gouvernementaux

Référence	Libellé exigence	Priorité
SECU_017	Dans le cadre de l'application de plans gouvernementaux, les autorités françaises peuvent décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications. Il peut également s'agir de mesures d'entraînement à la réaction en cas d'incident. Dans le cadre du marché, le titulaire peut être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le CNRS. Ces mesures sont susceptibles d'évoluer. Les modifications sont régulièrement transmises durant l'exécution du marché. Le titulaire est tenu de mettre immédiatement en œuvre lesdites dispositions, quand bien même elles auraient un impact significatif sur le coût de la prestation. Dans ce dernier cas, les conséquences financières de ces dispositions sont tirées soit par voie d'avenant, soit, en cas de désaccord persistant entre le CNRS et le titulaire, par les tribunaux compétents. Sans impact significatif sur les coûts, le respect de cette exigence est compris dans le prix des prestations du présent marché sans surcoût pour le CNRS.	0

6 ANNEXES

6.1 PRÉSENTATION DES DIRECTIONS DU CNRS CONCERNÉES

6.1.1 Le Secrétariat général du Comité national (SGCN)

Le **SGCN** assiste l'ensemble des instances et assure l'évolution des processus relevant de la mise en œuvre de leurs missions.

Par son soutien aux travaux du comité national (conseils, prospective, évaluation des chercheurs), le SGCN garantit le fonctionnement des instances et en accompagne les évolutions en lien avec la direction du CNRS, les instituts et les autres acteurs de la recherche scientifique.

Il a pour fonctions de :

- organiser les processus relatifs au conseil, à la prospective et à l'évaluation individuelle des chercheurs dans le respect de la réglementation,
- assurer le suivi des instances,
- assurer une veille juridique, réglementaire,
- diffuser les travaux du comité national,
- assurer la maîtrise d'ouvrage des systèmes d'information afférent aux processus.

Des informations plus complètes sont disponibles sur le site Web du SGCN à l'adresse suivante : http://www.cnrs.fr/comitenational/sgcn/accueil.htm

6.1.2 La direction générale déléguée aux ressources (DGD-R)

La **DGD-R** conduit, aux côtés du président, la politique administrative et financière de l'établissement. Elle a en charge le développement des ressources humaines et des activités de soutien à la recherche. Dans ce cadre, et en relation étroite avec la DGD-S, elle s'appuie sur les compétences des instituts du CNRS.

Pour remplir ses missions, la DGD-R s'appuie sur :

- dix-sept délégations régionales,
- six directions fonctionnelles,
- une structure transversale
- un pôle santé et sécurité au travail.

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

6.1.2.1 *La direction des affaires juridiques (DAJ)*

La **DAJ** assure une mission de conseil, d'expertise, de veille juridique et de défense de l'établissement.

Elle assure le secrétariat du conseil d'administration (CA) du CNRS et est chargée de l'organisation des processus électoraux concernant l'établissement.

Ses activités s'articulent autour de **6 pôles** :

- Pôle Accords Propriété Intellectuelle Valorisation (APIV)
- Pôle Ingénierie des Structures (IdS)
- Pôle Droit Public Economique et Réglementation (DPER)
- Pôle Responsabilité pénale et Maîtrise des Risques (RMR)
- Pôle Conseil d'administration, Ressources, Elections (CARE)
- Pôle National de Conservation des Données et Documents (PNC2D)

La direction anime également le **réseau des juristes du CNRS** (réseau e-loi).

6.1.2.2 *La direction des systèmes d'information (DSI)*

La **DSI** définit et met en œuvre les systèmes d'information de gestion et de pilotage des différentes activités du CNRS, en adéquation avec les orientations stratégiques et métiers de l'établissement (RH, finance, décisionnel, formation, référentiels, valorisation, missions…).

Elle gère également les outils mis en commun avec les partenaires du CNRS tels que l'Amue et les universités, ainsi que la sécurité des systèmes d'information (outils et services, animation du réseau des correspondants sécurité…).

Enfin, la DSI met à disposition des laboratoires une offre de services numériques (ODS) destinée à simplifier, soutenir et sécuriser leur quotidien (travail collaboratif, mobilité, services cloud, sauvegarde des données, exploitation sécurisée de sites internet…).

➢ La DSI comprend :

- **La Direction** : la directrice de la DSI est assistée d'un directeur adjoint et d'une directrice adjointe administrative.
- **Le Secrétariat Général** est chargé des aspects administratifs de la DSI. Il gère les ressources humaines, le budget, le contrôle de gestion, la logistique et les achats.
- **Le département SI Finance** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de BFC (budget, finance, comptabilité) et de l'Infocentre métier Finance, SI financiers du CNRS.
- **Le département SI Laboratoires et soutien à la recherche** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications à destination des laboratoires et des services centraux notamment pour la gestion des achats, la gestion des missions, le dialogue de gestion, la gestion du patrimoine immobilier, la gestion de la valorisation et les appels à projets. Il assure également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département SI Ressources humaines et paie** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de Sirhus (Système d'Information Ressources Humaines des Unités et Services du CNRS), de l'infocentre métier RH et des convertisseurs équivalent temps plein travaillé (ETPT).
- **Le département Solutions applicatives métiers et décisionnel** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications ressources humaines, santé, prévention, sécurité et décisionnel. Il réalise également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département Cybersécurité** met en œuvre la politique de sécurité des SI du CNRS pour l'ensemble des SI qui sont sous la responsabilité de la DSI. Il pilote et met en œuvre les démarches d'homologation de son périmètre. Il détermine les risques, objectifs et mesures de sécurité à intégrer dans les applications, services, outils, architectures et infrastructures. Il contrôle les mises en œuvre techniques et organisationnelles. Il définit, met en place et maintient les services de confiance numériques du CNRS. Il gère les incidents de sécurité de son périmètre. Il participe et collabore aux travaux de la CNSSI et de son centre de cyberdéfense.
- **Le département Plateforme des référentiels et de dématérialisation** met en œuvre les principaux référentiels structurants du SI. Il est chargé de les maintenir en conditions opérationnelles (plateforme MDM – Master Data Management). Il est aussi chargé de la mise en œuvre des plateformes de dématérialisation des documents, de préservation et de conservation de ces derniers (services de GED – Gestion Electronique de Documents et de SAE – Système d'Archivage Electronique).
- **Le département Architecture et assistance applicatives** met en place et maintient les annuaires et outils de gestion d'habilitations, fournit de l'assistance en termes d'expertise développement et architecture applicative. Il met en place et maintient les outils d'intégration des données et assure l'assistance utilisateurs.
- **Le département Infrastructures SI** est chargé de spécifier, mettre en œuvre, opérer et maintenir les infrastructures (notamment réseaux, systèmes, bases de données) du SI du CNRS. Il accompagne toutes les activités portées par la DSI dans le domaine des infrastructures et de l'exploitation technique.
- **Le département Sites web, communication, accompagnement projet** conçoit et met en œuvre les outils pour la communication et le travail collaboratif au sein du CNRS (intranet, portails, espaces collaboratifs, sites web). Il accompagne le déroulement des projets SI au niveau urbanisation (études pour l'intégration de nouveaux besoins), qualité-méthodes et ergonomie des technologies interface homme machine (IHM). Enfin, il a en charge la communication interne et externe de la DSI.

La DSI est implantée sur deux sites Toulouse-Labège (31) et Meudon (92).

Des informations plus complètes sont disponibles à l'adresse suivante : https://www.cnrs.fr/fr/dsi

6.1.2.3 *Direction de la sûreté (Dirsu)*

La **Dirsu** met en œuvre la politique de prévention et de maîtrise des risques d'atteintes volontaires aux personnes et au patrimoine matériel et immatériel au sein du CNRS.

Ses missions s'articulent étroitement avec les fonctions exercées par le Fonctionnaire de sécurité de défense (FSD). Le directeur de la sûreté est également Fonctionnaire de sécurité de défense du CNRS.

La direction comprend :

- Le responsable de la sécurité des systèmes d'information du CNRS (RSSIC) en tant que chargé de mission auprès du directeur de la sûreté pour le domaine de la sécurité de l'information et de la sécurité de l'information et de la sécurité des réseaux et systèmes d'information.
- Le conseiller national à la sécurité des transports de marchandises dangereuses (TMD) du CNRS chargé de recommander à toutes les entités du CNRS et, le cas échéant, à ses partenaires les actions et les procédures applicables aux transports de matières dangereuses. Il assure à ce titre une veille des réglementations internationales et nationales.
- Le conseiller pour l'intelligence économique qui est en charge de la mise en œuvre de la politique d'intelligence économique au CNRS dans le cadre de la politique nationale d'intelligence économique en lien avec les services compétents de l'État.

6.1.2.4 *Le Service Protection des Données (SPD)*

Le SPD assure la conformité du CNRS à la règlementation en matière de protection des données personnelles (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés).

Sous la responsabilité de la Déléguée à la protection des données, il conseille, assiste et contrôle le respect des dispositions prises par les entités en matière de protection des données personnelles.
Le SPD tient le registre des traitements et met à jour l'ensemble de la documentation liées à la protection des données personnelles.

6.2 ABRÉVIATIONS ET GLOSSAIRE

6.2.1 Abréviations

Le tableau suivant présente la liste des abréviations utilisées dans ce document.

Sigle	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface (interface de programmation applicative)
BAPI	Business Application Programming Interface
BDD	Base De Données
CAS	Central Authentication Service
CCAP	Cahier des Clauses Administratives Particulières
CCT	Cadre de Cohérence Technique
CCTP	Cahier des Clauses Techniques Particulières
CF	Comptabilité Finance
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre National de la Recherche Scientifique
CSS	Cascading Style Sheets
CSV	Comma-separated values
DAJ	Direction des Affaires Juridiques
DAO	Data Access Object (objet d'accès aux données)
DCP	Donnée à caractère personnel

Sigle	Description
DEV	plate-forme de DEVeloppement
DGD-R	Direction Générale Déléguée aux Ressources
DNS	Domain Name System (système de noms de domaine)
DROM-COM	Départements et régions d'Outre-mer et Collectivités d'Outre-mer
DSI	Direction des Systèmes d'Information
DU	Directeur d'Unité
EAI/ESB	Enterprise Application Integration (intégration d'applications d'entreprise) / Enterprise Service Bus
ETPT	Equivalent Temps Plein Travaillé
FOR	plate-forme de FORmation
FSD	Fonctionnaire de Sécurité de Défense
FTP	File Transfer Protocol (protocole de transfert de fichiers)
GED	Gestion Electronique de Documents
GIP	Groupement d'Intérêt Public
HTML	HyperText Markup Language (langage de balisage d'hypertexte)
HTTP	HyperText Transfer Protocol (protocole de transfert hypertexte)
HTTPS	HyperText Transfer Protocol Secure (protocole de transfert hypertexte sécurisé)
IdP	Identity Provider (fournisseur d'identité)
IHM	Interface Homme Machine
IPsec	Internet Protocol Security (protocole de sécurité internet)
IPv4	Internet Protocol version 4 (protocole internet version 4)
J2EE	Java 2 Enterprise Edition
JMS	Java Message Service
JSON	JavaScript Object Notation (format de données textuelles dérivé de la notation des objets du langage JavaScript)
JSR	Java Specification Request
LAN	Local Architecture Network (réseau local)
LDAP	Lightweight Directory Access Protocol (protocole d'accès aux annuaires)
MDM	Master Data Management (gestion des données de référence)
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
NAT	Network Address Translation (mécanisme de translation d'adresses)
NTP	Network Time Protocol (protocole d'heure réseau)
OS	Operating System
PGI	Progiciel de Gestion Intégré
PGSI	Politique Générale de Sécurité de l'Information
PAQ	Plan Assurance Qualité
PAS	Plan Assurance Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
PSST	Pôle Santé et Sécurité au Travail
REC	plate-forme de RECette
RENATER	REseau NAtional de télécommunications pour la Technologie, l'Enseignement et la Recherche

Sigle	Description
REST	REpresentational State Transfer
RFC	Requests For Comments (demande de commentaires)
RGAA	Référentiel général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
RSSIC	Responsable de la Sécurité des Systèmes d'Information du CNRS
SAE	Service d'archivage électronique
SAML	Security Assertion Markup Language (langage de balisage d'informations d'authentification)
SAN	Storage Area Network (réseau de stockage)
SGBD	Système de Gestion de Base de Données
SGCN	Secrétariat Général du Comité national
SHA	Secure Hash Algorithm
SI	Système d'Information
SMTP	Simple Mail Transfer Protocol (protocole simple de transfert de courrier)
SNMP	Simple Network Management Protocol (protocole simple de gestion de réseau)
SP	Service Provider (fournisseur de services)
SQL	Structured Query Language (langage de requête structurée)
SSH	Secure SHell
SSI	Sécurité des Systèmes d'Information
SSL	Secure Socket Layer
SSO	Single Sign-On (authentification unique)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network (réseau local virtuel)
VPN	Virtual Private Network (réseau privé virtuel)
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines (règles pour l'accessibilité des contenus Web)
XML	eXtensible Markup Language (langage de balisage extensible)
XSS	Cross Site Scripting

6.3 DÉTAIL DES SCRUTINS PAR INSTANCES POUR 2027

6.3.1 Élection pour le renouvellement des membres du CNESER

INSTANCE

Le CNESER est à la fois un organe consultatif placé auprès du ministre de l'enseignement supérieur, de la recherche et de l'espace. Le CNESER donne son avis sur les stratégies nationales de l'ESR. Il a également une fonction disciplinaire et statue en appel et dernier ressort sur les décisions disciplinaires prises par les instances universitaires compétentes à l'égard des enseignants-chercheurs, enseignants et usagers.

SCRUTIN

Les membres des collèges chercheurs et IT votent au scrutin de liste à la représentation proportionnelle au plus fort reste. sur un tour unique.

ELECTORAT

Le corps électoral est constitué d'électeurs inscrits par l'administration ou inscrits à leur demande.
Cela représente un potentiel d'environ 32 000 électeurs

ÉLIGIBILITE

Tout électeur est éligible dans son collège.

CANDIDATURES

Pour le collège chercheur : Les candidatures sont des candidatures de listes et sont toutes accompagnées d'une profession de foi et d'accords individuels de candidatures.

Pour le collège IT : Les candidatures doivent être rattachées à une liste. Les listes doivent être complètes et comprendre 4 candidats et 4 candidats suppléants. Chaque liste est accompagnée d'une profession de foi et d'accords individuels de candidatures.

MODALITES DE VOTE

Le vote a lieu à bulletin secret, uniquement par vote électronique.

6.3.2 Election pour le renouvellement des représentants du personnel aux Conseils scientifiques d'institut

INSTANCE

Le Conseil scientifique d'institut conseille et assiste par ses avis et ses recommandations le directeur de l'institut de manière prospective sur la pertinence et l'opportunité des projets et activités de l'institut. Pour aider le Conseil scientifique d'institut á assurer ses missions, des groupes de travail peuvent être constitués.

Il y a 10 instituts au CNRS, donc 10 Conseils scientifiques d'institut.

SCRUTIN

L'élection se déroule, par voie électronique, sur un tour :
Au scrutin plurinominal pour les électeurs des collèges A1, A2, B1 et B2.
Au scrutin de liste à la représentation proportionnelle et à la plus forte moyenne pour les électeurs du collège C.
12 membres élus répartis comme suit :

- 3 membres élus, par les personnels relevant du collège A1,
- 2 membres élus, par les personnels relevant du collège A2,
- 2 membres élus, par les personnels relevant du collège B1,
- 2 membres élus, par les personnels relevant du collège B2,
- 3 membres élus, par les personnels relevant du collège C.

ÉLECTORAT

Le corps électoral est constitué d'électeurs inscrits par l'administration ou inscrits à leur demande Le nombre d'électeurs est d'environ77 000.

CANDIDATURES

- **Pour le scrutin plurinominal :**
  Ce mode de scrutin concerne les collèges A1, A2, B1 et B2.
  Les candidatures sont individuelles.
- **Pour le scrutin de liste :**
  Ce mode de scrutin concerne uniquement le collège C.
  Les candidatures doivent être rattachées à une liste.

MODALITES DE VOTE

Le vote a lieu à bulletin secret, uniquement par vote électronique.

6.3.3 Election pour le renouvellement au Conseil scientifique

INSTANCE

Le Conseil scientifique veille à la cohérence de la politique scientifique du CNRS en liaison avec l'ensemble des instances scientifiques consultatives du Comité national

SCRUTIN

L'élection s'effectue selon un scrutin plurinominal majoritaire à un tour. Pour les électeurs des collèges A1, A2, B1 et B2 Les 11 membres à élire pour chaque CID sont répartis comme suit :

- 3 membres élus par les personnels relevant du collège A1,
- 2 membres élus par les personnels relevant du collège A2,
- 2 membres élus par les personnels relevant du collège B1,
- 2 membres élus par les personnels relevant du collège B2,
- - 2 membres élus par les personnels relevant du collège C.

ELECTORAT

Le corps électoral est constitué d'électeurs inscrits par l'administration. Il concerne des personnels CNRS et des personnels non CNRS.

Chaque électeur vote pour le CS et un CSI.

Les électeurs sont répartis en 5 collèges de vote : A1,A2,B1,B2 et C

ELIGIBILITE

Tout électeur est éligible, mais uniquement par le collège auquel il appartient.

CANDIDATURES

Pour les collèges A1,A2,B1 et B2 les candidatures sont individuelles et sont toutes accompagnées d'une profession de foi et d'une déclaration individuelle de candidature

Pour le collège C Les candidatures doivent être rattachées à une liste.

MODALITES DE VOTE

Le vote a lieu à bulletin secret, uniquement par vote électronique.