

Protocole d'Accord Préélectoral (PAP)

*Élections professionnelles UES
Orange 2023*

3 juillet 2023



Entre les soussignés :

Les sociétés Orange SA, 111 quai du Président Roosevelt, 92130 Issy-les-Moulineaux, Orange Caraïbe SA, 1 avenue Nelson Mandela, 94110 Arcueil et TOTEM France, 132 avenue de Stalingrad, 94800 Villejuif, représentées par Eric BOUSQUET, agissant en sa qualité de Directeur des Relations Sociales, et dûment mandaté à cet effet par chacune des sociétés ci-dessus nommées,

d'une part,

Et les Organisations Syndicales dûment mandatées et représentées respectivement par :

- pour la CDMT : **Christèle CRATER**

- pour la CFDT-F3C : **Sonia BANDERNE**

- pour la CFDT- PT : **Eddy PIERRE**

- pour la CFE-CGC ORANGE :

- pour la CFTC : **Pascal MAURY**

- pour la CGT- FAPT : **Samira GOUJA**

- pour la CGTG :

- pour la CGTR : **Vincent MUSANGER**

- pour la CGTM-P&T :

- pour la CTU :

- pour FOCOM : **Kaoutar SCHWIND**

- pour Orange Ensemble :

- pour Printemps Ecologique : **Dominique POITEVIN**

- pour le SNE :

- pour le STC : **Olivier HALTER**

- pour SUD-PTT : **Loic CARIOU**

- pour l'UNSA : **Jean-François LE BRAS**

- pour l'UTG :

- pour l'UTT UGTG :

- pour l'UGT M :

d'autre part.

SOMMAIRE

SOMMAIRE	4
Préambule	8
Chapitre 1 - Détermination et répartition des effectifs électoraux	9
Article 1 – Règles d’appréciation des effectifs	9
1.1 Les fonctionnaires	9
1.2 Les salariés de droit public et de droit privé	9
1.3 Les salariés mis à la disposition d’une société de l’UES par une entreprise sous-traitante et les intérimaires	10
1.4 Règles de prise en compte pour le calcul des effectifs	11
1.4.1 Personnels comptabilisés intégralement (pour 1 unité)	11
1.4.2 Personnels comptabilisés au prorata de leur durée de travail	11
1.4.3 Personnels comptabilisés au prorata de leur temps de présence	11
1.4.4 Salariés comptabilisés au prorata de leur durée de travail et au prorata de leur temps de présence	11
Article 2 – Date d’appréciation des effectifs et cadre géographique	12
2.1 Date d’appréciation des effectifs	12
2.2 Cadre géographique des élections CSE	12
Article 3 – Nombre et répartition du personnel dans les collèges électoraux	12
3.1 Nombre de collèges électoraux	12
3.2 Répartition du personnel dans les collèges électoraux	12
Chapitre 2 - Détermination et répartition des sièges dans les collèges électoraux	14
Article 4 – Détermination du nombre de sièges	14
Article 5 – Répartition des sièges entre les collèges électoraux	14
Chapitre 3 - Modalités de mise en place du CSEC : Répartition des sièges entre les CSE	15
Article 6 – Règles d’attribution et de répartition des sièges	15
6.1 Règles d’attribution des sièges	15
6.2 Règles de répartition des sièges restants	15
Chapitre 4 – Electorat et éligibilité	16
Article 7 – Conditions pour être électeur	16
7.1 Conditions communes aux fonctionnaires et aux salariés contractuels de l’UES	16
7.2 Les fonctionnaires électeurs	16

7.3	Les salariés contractuels électeurs.....	17
7.4	Les salariés mis à la disposition d'une société de l'UES par une entreprise sous-traitante	17
Article 8 - Listes électorales		17
8.1	Principes généraux.....	17
8.1.1	Listes électorales provisoires.....	18
8.1.2	Listes électorales rectifiées.....	19
8.1.3	Listes électorales définitives	19
Article 9 - Eligibilité		19
9.1	Conditions pour être éligible.....	19
Article 10 - Listes de candidats		20
10.1	Constitution des listes de candidats.....	20
10.2	Procédure de dépôt des listes de candidats	20
10.3	Affichage des listes de candidats	21
Chapitre 5 - Communication électorale		22
Article 11 – Information du personnel		22
11.1	Digitalisation de la communication électorale.....	22
11.1.1	Principes généraux	22
11.1.2	Communication électorale par messagerie électronique	22
11.1.3	Espace communication.....	22
11.2	Annonce des élections, vérification des listes électorales provisoires et modalités de vote	23
11.3	Information sur le matériel de vote	23
11.4	Information sur les candidatures	24
11.5	Ouverture du scrutin et relance des électeurs	24
Article 12 – Campagne électorale.....		24
12.1	Profession de foi	24
12.2	Logos et slogans.....	25
12.3	Communication syndicale	26
12.3.1	Panneaux d'affichage et tracts.....	26
12.3.2	Utilisation de la messagerie professionnelle.....	26
12.4	Moyens de campagne.....	27
12.4.1	Enveloppe financière.....	27
12.4.2	Crédit Temps Complémentaire (CTC)	27

12.4.3	Heures d'Information Syndicale (HIS).....	27
Chapitre 6 – Modalités pratiques du scrutin		29
Article 13 – Les bureaux de vote		29
13.1	Le bureau de vote centralisateur	29
13.2	Rôle du bureau de vote centralisateur	29
13.3	Les Bureaux de vote dits d' « Établissements Distincts »	30
13.4	Règles de désignation des membres des bureaux de vote	30
Article 14 – Modalités spécifiques de l'élection par voie électronique		31
14.1	Principes généraux.....	31
14.2	Protection des données personnelles.....	32
14.3	Le scrutin électronique	32
14.3.1	Période du scrutin.....	32
14.3.2	Le site de vote	32
14.3.3	Les lieux du scrutin	33
14.4	Sécurisation du vote électronique	33
14.4.1	Validation des écrans pour les bulletins de vote électronique	33
14.4.2	Matériel de vote électronique.....	33
14.4.3	Scellement des urnes électroniques	34
	La quatrième et dernière étape est le scellement des urnes.....	35
14.5	Déroulement du vote électronique : le parcours électeur [à valider avec prestataire].....	35
14.5.1	Etape 1 : connexion au site de vote et authentification	35
14.5.2	Etape 2 : Choix du vote.....	36
14.5.3	Etape 3 : Validation du vote	36
14.6	Données consultables pendant le scrutin	36
Article 15 - Les bulletins de vote		37
Article 16 - Assistance Hotline		37
Article 17 – Dépouillement		38
17.1	Contrôles préalables et descellement des urnes électroniques	38
17.2	Déroulement du dépouillement	38
Article 18 – Proclamation et publicité des résultats.....		39
18.1	Procès-verbaux CERFA	39
18.2	Proclamation des résultats	39
18.3	Affichage des résultats.....	40

18.4	Transmission des résultats concernant les salariés de droit privé au Ministère du travail (MARS)	40
18.5	Attribution des sièges.....	40
18.6	Communication des résultats détaillés aux Organisations Syndicales.....	40
Chapitre 7 – Dispositions finales		41
Article 19 – Durée de l'accord.....		41
Article 20 – Modalités de révision.....		41
Article 21 – Notification et formalités de dépôt		41
Annexe n°1 - Détermination du nombre de sièges par établissements distinct (CSEE), et répartition des sièges entre les collègues		44
Annexe n°2 - Répartition des sièges du CSEC		46
Annexe n°3 - Planning du 1^{er} tour du scrutin CSE du 13 au 16 novembre 2023.....		47
Annexe n° 4 - Planning du 2nd tour éventuel du scrutin CSE du 27 au 29 novembre 202350		
Annexe n° 5 - Cahier des charges de mise en œuvre du vote électronique pour les élections CSE 2019.....		52

Préambule

Le Protocole d'Accord Préélectoral (PAP) fixe les modalités d'organisation et de déroulement des opérations électorales. Ces éléments doivent être définis dans le respect des principes généraux du droit électoral, conformément à l'article L. 2314-28 du code du travail.

Les élections CSE 2023 au sein de l'Unité Economique et Sociale (UES) Orange se tiendront :

- **du 13 au 16 novembre 2023 pour le 1^{er} tour ;**
- **du 27 au 29 novembre 2023 pour l'éventuel 2nd tour.**

Le présent accord est destiné à préciser les modalités pratiques de ces élections pour la mandature CSE 2023 au sein de l'UES Orange, telle que définie par l'accord du 12 décembre 2022.

Les 18 Organisations Syndicales Intéressées suivantes ont participé à au moins une réunion de négociation du Protocole d'Accord Préélectoral : la CDMT, la CFDT-F3C, la CFDT- PT, la CFE-CGC ORANGE, la CFTC, la CGT- FAPT, la CGTG, la CGTR, la CGTM-P&T, FOCom, Orange Ensemble, Printemps Ecologique, STC, SUD PTT, l'UNSA, l'UTG, l'UTT UGTG et l'UGT M.

Chapitre 1 - Détermination et répartition des effectifs électoraux

Article 1 – Règles d’appréciation des effectifs

1.1 Les fonctionnaires

Sont pris en compte dans les effectifs d’assujettissement, les fonctionnaires de l’UES :

- en activité dans l’UES, à temps plein ou à temps partiel, y compris ceux en télétravail ;
- en congé : annuel, de maladie, de longue maladie, de longue durée, pour maternité ou, pour adoption, de paternité, en congé parental, en congé de formation professionnelle ou de formation syndicale, dans le cadre d’un compte épargne temps, pour période d’instruction militaire, en congé de solidarité familiale ;
- en mission ;
- mis à disposition :
 - a. au sein de l’UES : les fonctionnaires sont comptabilisés dans l’Établissement Distinct utilisateur ;
 - b. en dehors de l’UES : les fonctionnaires sont comptabilisés dans l’Établissement Distinct de Gestion ;
- détachés au sein d’Orange SA ou d’une filiale de l’UES ;
- en TPS/TPA ;
- en suspension de fonctions dans le cadre d’une procédure disciplinaire.

Sont exclus des effectifs d’assujettissement les fonctionnaires :

- détachés hors de l’UES, soit au titre de l’article 14 du décret n°85-986 du 16 septembre 1985, soit détaché dans une filiale n’appartenant pas à l’UES ;
- en disponibilité ;
- hors cadre à l’extérieur d’Orange SA.

1.2 Les salariés de droit public et de droit privé

Sont pris en compte dans les effectifs d’assujettissement :

- les salariés de droit privé titulaires d’un Contrat à Durée Indéterminée (CDI) ou d’un Contrat à Durée Déterminée (CDD), à temps plein ou à temps partiel, y compris ceux en télétravail ;
- les salariés dont le contrat de travail est suspendu ;
- les salariés en TPS/TPA ;
- les agents contractuels de droit public.

Sont exclus des effectifs d'assujettissement :

- les apprentis et les salariés titulaires d'un contrat de professionnalisation ;
- les salariés remplaçant une personne absente ;
- les salariés remplaçant une personne dont le contrat de travail ou le lien statutaire est suspendu ;
- les titulaires d'un contrat initiative-emploi, pendant la durée d'attribution de l'aide financière mentionnée à l'article L. 5134-72 du code du travail.

1.3 Les salariés mis à la disposition d'une société de l'UES par une entreprise sous-traitante et les intérimaires

Conformément à l'article L. 1111-2 du code du travail, doivent être pris en compte dans les effectifs d'assujettissement :

- les salariés mis à la disposition d'une société de l'UES par une entreprise extérieure qui sont physiquement présents dans les locaux de cette société utilisatrice et y travaillent depuis au moins un an ;
- les intérimaires, sauf s'ils remplacent un membre du personnel de l'UES absent ou dont le contrat de travail ou le lien statutaire est suspendu,

Ces salariés sont pris en compte dans les effectifs d'assujettissement à due proportion de leur temps de présence au cours des douze mois précédant le premier jour des élections défini dans le présent accord.

Les salariés mis à disposition par une société sous-traitante susceptible d'entrer dans ce décompte sont exclusivement :

- les salariés effectuant le gardiennage des bâtiments et le personnel d'accueil ;
- les salariés chargés du courrier s'ils sont présents dans les locaux de l'entreprise ;
- le personnel médico-social présent dans les locaux de l'entreprise ;
- le personnel technique présent dans les répartiteurs de l'entreprise ;
- les salariés effectuant le nettoyage des locaux de l'entreprise ;
- les informaticiens (pratiquement tous types de métiers et notamment des ingénieurs informaticiens, chefs de projet, analystes programmeurs, pilotes d'applications, concepteurs, intégrateurs, développeurs, ingénieurs d'exploitation, administrateurs bases de données...) travaillant dans les locaux de l'entreprise ;
- les salariés chargés d'affaires dans les Unités d'Intervention ;
- les salariés des entreprises de travaux de réseaux réalisant des travaux et prestations soit dans nos locaux soit sur nos ouvrages (travaux réseaux et interventions sur site).

1.4 Règles de prise en compte pour le calcul des effectifs

1.4.1 Personnels comptabilisés intégralement (pour 1 unité)

Sont comptabilisés pour 1 Equivalent Temps Plein (ETP) :

- les personnels de l'UES titulaires d'un Contrat de travail à Durée Indéterminée (CDI), y compris pendant une période d'essai ou de préavis, et les fonctionnaires, dès lors qu'ils travaillent à temps plein, qu'ils soient présents dans l'UES ou dont le contrat de travail ou le lien statutaire est suspendu, notamment en raison d'une formation qu'ils suivent ;
- les Cadres Exécutifs Autonomes (CEA).

1.4.2 Personnels comptabilisés au prorata de leur durée de travail

Les personnels de l'UES titulaires d'un Contrat de travail à Durée Indéterminée et les fonctionnaires à temps partiel, y compris TPS/TPA, sont comptabilisés au prorata de leur durée de travail.

1.4.3 Personnels comptabilisés au prorata de leur temps de présence

Sont comptabilisés au prorata de leur temps de présence au cours des 12 derniers mois précédant la date d'appréciation des effectifs définie à l'article 2 du présent accord, sous réserve qu'ils ne remplacent pas un membre du personnel de l'UES absent ou dont le contrat de travail ou le lien statutaire est suspendu :

- les salariés en Contrat à Durée Déterminée (CDD) ;
- les intérimaires ;
- les salariés mis à la disposition d'une société de l'UES par une entreprise sous-traitante tels que définis à l'article 1.3.

1.4.4 Salariés comptabilisés au prorata de leur durée de travail et au prorata de leur temps de présence

Sont comptabilisés au prorata de leur durée de travail et au prorata de leur temps de présence, sous réserve qu'ils ne remplacent pas un membre du personnel de l'UES absent ou dont le contrat de travail ou le lien statutaire est suspendu :

- les salariés en Contrat à Durée Déterminée (CDD) à temps partiel ;
- les intérimaires à temps partiel.

Article 2 – Date d’appréciation des effectifs et cadre géographique

2.1 Date d’appréciation des effectifs

Les effectifs internes et sous-traitants pris en compte dans le cadre du présent accord sont ceux arrêtés à la date du **31 janvier 2023**.

2.2 Cadre géographique des élections CSE

Les Etablissements Distincts CSE sont définis dans l’avenant n°3 à l’accord portant sur le dialogue social du 13 mai 2019.

Article 3 – Nombre et répartition du personnel dans les collèges électoraux

3.1 Nombre de collèges électoraux

Conformément aux dispositions de l’article L. 2314-11 du code du travail, le nombre de collèges électoraux est fixé à 3 pour chaque scrutin CSE.

3.2 Répartition du personnel dans les collèges électoraux

Au niveau de chaque Établissement Distinct, les parties conviennent de répartir les personnels comme suit :

1^{er} collège Employés, ouvriers	2^{ème} collège Techniciens, agents de maîtrise	3^{ème} collège Ingénieurs, chefs de services, cadres administratifs, commerciaux ou techniques assimilés sur le plan classification
I.1 à II.2 inclus et A à C inclus	II.3 et D	III.2 à IV.6 et Dbis à G

Pour l'Etablissement Distinct TOTEM France, les parties conviennent de répartir les personnels comme suit :

1^{er} collègue Employés, ouvriers Non Représenté	2^{ème} collègue Techniciens, agents de maitrise	3^{ème} collègue Ingénieurs, chefs de services, cadres administratifs, commerciaux ou techniques assimilés sur le plan classification
sans objet	D	E à G

Chapitre 2 - Détermination et répartition des sièges dans les collèges électoraux

Article 4 – Détermination du nombre de sièges

Le nombre de CSE est défini dans l'avenant n°3 à l'accord portant sur le dialogue social du 13 mai 2019. Le nombre de sièges affecté à chacun de ces CSEE figure en annexe 1 du présent accord.

Article 5 – Répartition des sièges entre les collèges électoraux

La répartition des sièges entre les collèges électoraux figure en annexe 1 du présent accord.

Sauf exception, cette répartition est réalisée proportionnellement à l'effectif constaté pour chacun des collèges et l'attribution des sièges restants au plus fort reste.

Chapitre 3 - Modalités de mise en place du CSEC : Répartition des sièges entre les CSE

Conformément aux dispositions de l'accord du 13 mai 2019 portant sur le « dialogue social au sein de l'UES Orange, à défaut d'accord entre les OS dans un délai de 3 semaines suivant la proclamation des résultats des élections professionnelles, le présent accord a pour objet de déterminer la répartition des sièges au niveau du CSE Central entre les différents Comités Sociaux et Economiques d'Etablissements (CSEE) pour la mandature issue des élections professionnelles de 2023.

Article 6 – Règles d'attribution et de répartition des sièges

6.1 Règles d'attribution des sièges

Le CSE Central est composé de 25 titulaires de 25 suppléants.

Les parties conviennent d'attribuer dans un premier temps :

- un siège de titulaire au CSEC à chacun des 15 CSEE composant l'UES Orange et définis dans l'avenant n°3 à l'accord portant sur le dialogue social du 13 mai 2019, soit 15 sièges de titulaires ;
- un siège de suppléant aux CSEE dont les effectifs ETP sont au moins égal à 1 400. Les ETP pris en compte sont ceux arrêtés à la date du 31 janvier 2023, tels que reportés dans l'annexe 2.

Selon cette règle de répartition, 15 sièges de titulaires et 12 sièges de suppléants sont attribués.

6.2 Règles de répartition des sièges restants

Les parties conviennent d'attribuer dans un second temps les 23 sièges restants (10 titulaires et 13 suppléants) comme suit :

Dans un premier temps les 10 sièges de titulaires aux 10 CSE dont les ETP sont au moins égaux à 1 400 ETP et dont les effectifs (ETP) sont les plus importants, puis les 13 sièges de suppléants selon l'ordre décroissant des effectifs (ETP) des CSEE.

Le nombre de sièges supplémentaires attribué à chaque CSEE en application de cette règle de répartition figure en annexe 2 du présent accord.

Chapitre 4 – Electorat et éligibilité

Article 7 – Conditions pour être électeur

Les conditions énumérées ci-après s'apprécient à la date du 1^{er} tour du scrutin et restent valables pour l'éventuel 2nd tour.

7.1 Conditions communes aux fonctionnaires et aux salariés contractuels de l'UES

Sont électeurs les personnels de l'UES cités dans les articles 7.2 et 7.3 ci-après :

- présents à l'effectif de l'UES à la date du 1^{er} tour du scrutin ;
- âgés de 16 ans révolus ;
- jouissant de leurs droits civiques ;
- travaillant depuis 3 mois au moins au sein du Groupe Orange.

Sont exclus de l'électorat les mandataires sociaux non liés par un contrat de travail avec les sociétés de l'UES Orange. A ce titre, le Président du Conseil d'Administration et la Directrice Générale d'Orange ne sont pas admis à participer à ce scrutin.

7.2 Les fonctionnaires électeurs

Sont électeurs, les fonctionnaires de l'UES qui remplissent les conditions rappelées à l'article 7.1 et qui sont :

- en activité dans l'UES, à temps plein ou à temps partiel, y compris ceux en télétravail ;
- en congé : annuel, de maladie, de longue maladie, de longue durée, pour maternité ou pour adoption, parental d'éducation, de paternité, en congé de formation professionnelle ou de formation syndicale, dans le cadre d'un compte épargne temps, pour période d'instruction militaire, en congé de solidarité familiale ;
- en mission ;
- mis à disposition au sein d'une filiale d'Orange : ces fonctionnaires seront électeurs au sein de l'Établissement Distinct de gestion, sauf s'ils ont choisi d'exercer leur droit de vote dans leur entreprise d'accueil ;
- détachés au sein d'Orange SA ou d'une filiale de l'UES : ces fonctionnaires seront électeurs dans l'Établissement Distinct d'accueil, étant liés par un contrat de travail de droit privé avec la société d'accueil, ils voteront dans l'urne « salariés de droit privé » au 1^{er} tour CSE titulaire ;
- en TPS/TPA ;
- en suspension de fonctions dans le cadre d'une procédure disciplinaire.

Sont exclus de l'électorat les fonctionnaires :

- détachés hors de l'UES, soit au titre de l'article 14 du décret n°85-986 du 16 septembre 1985, soit détachés dans une filiale n'appartenant pas à l'UES ;
- en disponibilité ;
- hors cadre à l'extérieur d'Orange SA.

7.3 Les salariés contractuels électeurs

Sont électeurs les salariés contractuels de l'UES qui remplissent les conditions rappelées à l'article 7.1 et qui sont :

- salariés de droit privé titulaires d'un Contrat à Durée Indéterminée (CDI) ou en Contrat à Durée Déterminée (CDD), à temps plein ou à temps partiel, y compris ceux en télétravail ;
- salariés dont le contrat de travail est suspendu ;
- les apprentis et les salariés titulaires d'un contrat de professionnalisation ;
- salariés de droit privé en TPS/TPA ;
- agents contractuels de droit public.

Par ailleurs, pour les CDD, les 3 mois d'ancienneté peuvent être atteints par cumul de la durée de contrats à durée déterminée successifs ou discontinus.

7.4 Les salariés mis à la disposition d'une société de l'UES par une entreprise sous-traitante

Sont électeurs par principe au sein de l'UES les salariés mis à disposition par une entreprise sous-traitante, qui remplissent les conditions mentionnées à l'article 1.3 du présent accord, ainsi que les conditions d'âge et de capacité électorale visées à l'article 7.1 du même protocole, et qui sont présents dans la société utilisatrice depuis au moins douze mois continus.

Ces salariés devront cependant choisir s'ils exerceront leur droit de vote, pour les élections CSE dans l'entreprise qui les emploie ou dans la société utilisatrice de l'UES. La date butoir pour effectuer ce choix est fixée au **lundi 4 septembre 2023**.

S'ils choisissent la société utilisatrice, cette dernière affectera alors chacun de ces salariés dans le collège électoral *ad hoc* en fonction de l'équivalence CCNT en vigueur chez Orange.

Article 8 - Listes électorales

8.1 Principes généraux

Dans le cadre de la fiabilisation des listes électorales, la date de gel des mouvements collectifs est fixée au **31 juillet 2023** pour les élections professionnelles de novembre 2023.

Les listes électorales seront établies par collège et comporteront les indications suivantes :

- nom ;
- prénom ;
- civilité ;
- date d'entrée dans le Groupe ;
- année de naissance.

Elles seront affichées en version provisoire, rectifiée, puis définitive en cas de réclamations d'électeurs :

- dans l'espace communication du prestataire de vote électronique ;
- au siège administratif de chaque Établissement Distinct ;

Par exception, l'affichage sera réalisé au sein du site majoritaire en termes d'effectif de chaque département administratif pour les Départements et Régions d'Outre-Mer (DROM).

En plus des indications données sur les Intranets et par push mails, les lieux et moyens de consultation des listes électorales seront précisés par voie d'affichage papier au siège de chaque Établissement Distinct, dans les mêmes conditions.

Chaque Organisation Syndicale aura la possibilité de consulter les listes électorales sur le site de supervision du prestataire de vote électronique avant le premier affichage et bénéficiera à ce titre de 50 habilitations sur le site de supervision.

Pour des raisons de protection des données à caractère personnel, les Organisations Syndicales habilitées utiliseront ces données uniquement aux fins de contrôle de l'électorat. Elles ne devront en aucun cas les diffuser à qui que ce soit et sous quelque forme que ce soit. Dans ce cadre aucun téléchargement ne sera possible sur la plateforme de consultation.

Afin de procéder à l'affichage précité et de réaliser un traitement électronique des votes, les listes électorales sont également transmises au prestataire de vote électronique

8.1.1 Listes électorales provisoires

Les listes électorales provisoires seront affichées le **mardi 10 octobre 2023 avant 14 heures** (heure de Paris).

Un courrier sera envoyé à chaque électeur à son domicile pour le lundi 9 octobre 2023. Le contenu de ce courrier est précisé à l'article 11.2 du présent accord.

Chaque jour et ce, jusqu'à la date limite de réclamation fixée au **vendredi 13 octobre 2023 à midi** (heure de Paris), le prestataire transmettra à l'employeur l'ensemble des réclamations signalées à la hotline afin qu'elles soient traitées par les Responsables Ressources Humaines compétents sur le périmètre de rattachement de l'électeur.

Le prestataire conservera la trace de tous les appels de réclamation pour modification des listes électorales provisoires.

Il sera procédé, le cas échéant, à la correction de ces listes provisoires. Une réponse sera apportée à toute réclamation.

8.1.2 Listes électorales rectifiées

Une fois le délai de réclamation des listes électorales provisoires achevé, les listes électorales rectifiées seront affichées le **mardi 17 octobre 2023 avant 14 heures** (heure de Paris) à la place des listes provisoires.

Elles ne pourront plus être modifiées qu'en application d'une décision de justice.

Les électeurs disposeront alors d'un délai de 3 jours pour se pourvoir devant les tribunaux, soit jusqu'au **vendredi 20 octobre 2023** au plus tard.

8.1.3 Listes électorales définitives

Si les listes électorales ont fait l'objet d'un ou de plusieurs recours judiciaires, elles seront affichées dans leur version finale le **lundi 23 octobre à 14 heures** (heure de Paris).

Les listes électorales ainsi affichées vaudront pour l'éventuel 2nd tour du scrutin.

Article 9 - Eligibilité

9.1 Conditions pour être éligible

Conformément à l'article L. 2314-19 du code du travail, sont éligibles dans le cadre des élections CSE, les personnels électeurs visés aux articles 7.1, 7.2, 7.3 du présent accord, ayant à la date du 1^{er} tour de scrutin :

- 18 ans révolus ;
- travaillé depuis un an au moins dans le Groupe Orange.

Sont ainsi exclues de l'éligibilité toutes les personnes représentant l'employeur auprès des CSE (cette exclusion ne vise pas les personnes qui présentent les dossiers dans les CSE) et celles disposant du pouvoir d'embaucher et de sanctionner les membres du personnel.

Seront notamment obligatoirement exclus :

- les Directeurs Orange et Directeurs des Divisions ;
- les DRH des Directions Orange, les DRH des Directions Métiers et les DRH des Divisions ;
- les Directeurs d'Unité Orange, du fait de leurs délégations d'autorité, lorsque celles-ci les placent régulièrement en position d'employeur.

Article 10 - Listes de candidats

10.1 Constitution des listes de candidats

La composition des listes se fait librement sans que le nombre de candidats ne dépasse le nombre de sièges à pourvoir. Les listes incomplètes sont admises.

Ces listes seront distinctes pour chacun des collèges et séparées pour les titulaires et les suppléants.

Conformément aux dispositions du code du travail, la direction communiquera la répartition femmes/hommes des listes électorales aux organisations syndicales aux fins de constitution de leurs listes de candidats.

Compte tenu de la date d'établissement des listes électorales, cette répartition sera annexée au présent accord à partir de septembre 2023. La direction s'engage néanmoins à fournir en amont et pour information aux Organisations Syndicales la répartition femmes/hommes des effectifs de l'UES au 31 janvier 2023, tels que définis dans le présent accord.

10.2 Procédure de dépôt des listes de candidats

Les listes de candidats seront déposées auprès du service Ressources Humaines de chaque Établissement Distinct. Un délégué de liste ou, en cas d'absence, son suppléant, qui aura reçu mandat exprès de toute personne habilitée par l'organisation syndicale à délivrer ce type de mandat au regard des statuts, pourra déposer une liste.

En cas de liste commune, la répartition des voix entre les Organisations Syndicales ayant déposé la liste sera précisée sur cette liste. A défaut, la répartition des voix s'effectuera au prorata du nombre d'Organisation Syndicale présente sur la liste.

Les listes peuvent être communiquée par tout moyen écrit avec preuve du dépôt (récépissé, LR + AR, courriel avec accusé de lecture, etc.).

Il est rappelé que le 1^{er} tour est réservé aux organisations syndicales et que les candidatures sont libres en cas d'organisation d'un 2nd tour.

Il est en outre rappelé qu'une Organisation Syndicale n'est pas tenue de déposer une nouvelle liste pour l'éventuel 2nd tour lorsque celle-ci est identique à celle déposée pour le 1^{er} tour. Dans l'hypothèse où cette liste serait différente de celle présentée au premier tour, elle en informera simplement la direction par une personne dûment mandatée par écrit (courrier ou courriel) dans les mêmes délais que définis ci-après.

Par ailleurs, afin d'éviter tout litige sur les listes des candidats et les listes des électeurs, les parties conviennent que celles-ci ne tiendront pas compte des promotions réalisées après le 6 octobre 2023.

Ainsi, les listes de candidats seront traitées en appréciant la situation administrative des effectifs au regard des collèges électoraux à la date du 6 octobre 2023.

La date limite de dépôt des candidatures est fixée au **lundi 23 octobre 2023 avant midi** (heure locale) pour le 1^{er} tour de scrutin et au **mardi 21 novembre 2023 avant midi** (heure locale) pour l'éventuel 2nd tour. Aucune liste ne peut être déposée après ces dates.

Au niveau de l'Établissement Distinct, les directions désigneront des personnes habilitées à recevoir ces listes. Les coordonnées de ces personnes seront communiquées aux Organisations Syndicales au plus tard le 29 septembre 2023.

10.3 Affichage des listes de candidats

Les listes de candidats seront affichées sur l'espace communication du prestataire de vote électronique et au siège de chaque Établissement Distinct :

- le **mardi 31 octobre 2023 avant 14 heures** (heure locale) pour le 1^{er} tour ;
- le **jeudi 23 novembre 2023 avant 14 heures** (heure de locale) pour le 2nd tour.

Chapitre 5 - Communication électorale

Article 11 – Information du personnel

11.1 Digitalisation de la communication électorale

11.1.1 Principes généraux

Les élections des représentants du personnel aux CSE se dérouleront exclusivement par voie électronique.

Chaque salarié aura accès aux informations indispensables aux élections via son intranet ou, à défaut, par push mail. Les articles intranet resteront en ligne pendant toute la durée des élections.

Le prestataire de vote électronique aura par ailleurs en charge une partie de la diffusion de la communication électorale émanant de la direction.

La date des élections et le numéro de la hotline prévue à l'article 16 du présent accord seront précisés dans toutes les communications.

11.1.2 Communication électorale par messagerie électronique

Par principe, les communications électorales seront envoyées par l'entreprise sur la messagerie professionnelle.

Par exception, les personnels éloignés du service pourront se rapprocher de leur service RH afin de leur communiquer une adresse de messagerie personnelle sur laquelle leur adresser la communication électorale. Cette possibilité leur sera indiquée dans le 1^{er} courrier prévu à l'article 11.2 du présent accord.

11.1.3 Espace communication

Un espace communication sera réservé sur le site de vote dès le 10 octobre 2023.

Les salariés, électeurs ou non, pourront y consulter les listes électorales provisoires et rectifiées.

Les électeurs pourront y consulter :

- les informations générales relatives au vote et ses modalités ;
- la propagande électorale ;
- les listes électorales définitives ;
- les listes de candidats dans l'ordre du tirage au sort, prévu à l'article 12.3.1 du présent accord.

11.2 Annonce des élections, vérification des listes électorales provisoires et modalités de vote

L'annonce des élections au personnel de l'UES Orange sera réalisée le **mardi 10 octobre 2023** sur l'Intranet Anoo.

Un premier courrier sera envoyé à chaque électeur dans la semaine du 25 septembre 2023 pour les DROM et la DRR Corse et la semaine du 2 octobre 2023 pour la France Hexagonale (réception pour le 9 octobre), comportant les informations suivantes :

- la date des élections ;
- l'extrait de la liste électorale lui permettant de vérifier les données qui le concernent, comme précisé à l'article 8.1.1 du présent accord. Les électeurs seront expressément invités à vérifier leur bonne inscription sur les listes électorales provisoires, étant rappelé que l'employeur doit mettre chaque électeur en capacité de faire ces vérifications ;
- le numéro d'appel de la hotline organisée par le prestataire de vote électronique prévue à l'article 16 du présent accord, qui sera mise à disposition des électeurs afin d'exprimer leurs réclamations ;
- les informations relatives aux modalités de vote ;
- les modalités pour demander à se faire expédier à une adresse électronique de son choix l'ensemble de la communication des élections faite par push mail, pour tout salarié éloigné du service (congé maladie, TPS/TPA ...).

Ce courrier intervient en plus de l'affichage des listes électorales prévu à l'article 8 du présent accord.

Un push mail annonçant la date des élections, les modalités de vote, le numéro de la hotline et indiquant le lien vers les listes électorales sera également envoyé à tout le personnel de l'UES Orange, électeur ou non, le mardi 10 octobre 2023.

En plus des indications données par voie électronique, les lieux et moyens de consultation des listes électorales seront en tout état de cause précisés par voie d'affichage papier au niveau de chaque siège d'Établissement Distinct.

Un push mail annonçant la date du 2nd tour sera envoyé à tous les électeurs concernés, le cas échéant.

11.3 Information sur le matériel de vote

Chaque électeur dispose d'un identifiant unique et d'un mot de passe valables pour le scrutin.

Pour le 1^{er} tour, un second courrier sera envoyé à chaque électeur la semaine du 30 octobre 2023 pour les DROM et la DRR Corse et la semaine du 6 novembre 2023 pour la France Hexagonal (réception pour le 10 novembre), comportant les informations suivantes :

- l'identifiant unique de connexion ;
- le numéro d'appel de la hotline organisée par le prestataire de vote électronique prévue à l'article 16, qui sera mise à disposition des électeurs afin d'exprimer leurs réclamations ;
- les informations relatives aux modalités de vote ;

- une notice de vote.

Grâce à son identifiant, l'électeur crée lui-même son mot de passe sur le site de vote selon la procédure sécurisée décrite à l'article 14.4.2.

En tout état de cause, il sera possible se connecter à un espace sécurisé dès l'ouverture de la période de vote, permettant ainsi de récupérer un nouveau matériel de vote personnel.

Cet espace sécurisé sera accessible à partir d'un lien figurant dans les push mails envoyés par la direction au début et pendant le scrutin.

En cas de 2nd tour, chaque électeur pourra récupérer son matériel de vote via cet espace sécurisé, accessible à partir d'un lien figurant dans le push mail envoyé par la direction au début et pendant le 2nd tour.

11.4 Information sur les candidatures

Les électeurs seront informés des différentes candidatures pour le 1^{er} tour au moyen de deux push mails envoyés prévus à l'article 12.1 du présent accord et envoyés par la direction.

Un autre push mail sera envoyé entre les deux tours, le cas échéant.

Cette information intervient en plus de l'affichage des listes de candidats prévu à l'article 10.3 du présent accord.

Un push mail indiquant le lien vers les listes de candidats sera également envoyé aux électeurs le **mardi 31 octobre 2023** pour le 1^{er} tour et le **jeudi 23 novembre 2023** pour l'éventuel 2nd tour.

11.5 Ouverture du scrutin et relance des électeurs

La direction enverra un push mail à chaque électeur **le lundi 13 novembre 2023 entre 14 heures et 16 heures** (heure de Paris) pour annoncer l'ouverture du vote qui contiendra un lien pour accéder au site de vote.

Un ou plusieurs push mails seront également envoyés au cours de la période de vote aux fins de rappeler l'importance du scrutin. Ils ne contiendront pas les professions de foi.

L'ouverture de la période de vote sera également annoncée sur l'Intranet.

Cette procédure sera répétée en cas de 2nd tour.

Article 12 – Campagne électorale

12.1 Profession de foi

Une profession de foi nationale devra être déposée à la Direction des Relations Sociales Groupe et une profession de foi locale personnalisable par Établissement Distinct devra être déposée aux services Ressources Humaines de chaque Établissement Distinct :

- par chaque Organisation Syndicale ayant déposé une liste au plus tard **le lundi 23 octobre 2023 avant midi** (heure locale) ;
- par chaque Organisation Syndicale ayant déposé une liste ou chaque liste de candidats libres au plus tard le **mardi 21 novembre 2023 avant midi** (heure locale) pour l'éventuel 2nd tour.

Chaque profession de foi doit être communiquée sous format PDF, avec un poids préconisé de 500 KO à 2 mégas.

Elles seront consultables dans l'espace communication prévu à l'article 11.1.3 du présent accord, puis sur le site de vote, au moment du choix de l'électeur, aux côtés des listes de candidats afférentes.

Les coordonnées des personnes habilitées à recevoir les professions de foi seront communiquées aux organisations syndicales en amont du dépôt des listes.

La direction enverra par ailleurs deux push mails aux électeurs avant le scrutin : **jeudi 2 novembre 2023** et le **vendredi 10 novembre 2023**.

La propagande ainsi envoyée pourra être différente de celle communiquée le 23 octobre et, le cas échéant, devra être envoyée à la Direction des Relations Sociales Groupe le **vendredi 27 octobre 2023** au plus tard.

En cas de 2nd tour, un autre push mail sera envoyé entre les deux tours du scrutin.

Ces push mails permettront à chaque électeur de consulter les professions de foi des Organisations Syndicales.

Les push mails envoyés pendant la période de vote ne contiendront pas les professions de foi.

Le tirage au sort évoqué à l'article 12.3.1 permet également de déterminer l'ordre d'apparition des professions de foi et des listes associées sur le site de vote et sur les push mails.

Au niveau de l'Établissement Distinct, les directions désigneront des personnes habilitées à recevoir ces professions de foi. Les coordonnées de ces personnes seront communiquées aux Organisations Syndicales au plus tard le 29 septembre 2023.

12.2 Logos et slogans

Les logos et slogans qui seront utilisés sur le site de vote devront être communiqués à la Direction des Relations Sociales Groupe le plus en amont possible, et au plus tard au jour le **lundi 9 octobre 2023**.

Ils devront répondre aux caractéristiques suivantes :

- Format : png ;
- Taille : carré de 200 pixels sur 200 pixels ;
- Charte graphique : **l'utilisation des logos d'Orange n'est pas autorisée.**

Les slogans ne pourront pas excéder une longueur de 128 caractères (espaces compris).

12.3 Communication syndicale

Les principes ci-dessous énoncés ont pour objectif de rappeler l'état des dispositions applicables, dont le non-respect peut entraîner une contestation des opérations électorales.

La communication électorale s'effectue dans le cadre des dispositions légales et conventionnelles en vigueur à l'UES Orange.

12.3.1 Panneaux d'affichage et tracts

Conformément aux dispositions du code du travail, les moyens d'information à la disposition des candidats sont l'affichage et la distribution de tracts.

Des panneaux d'affichage, habituellement dévolus à la direction et/ou mis en place spécifiquement pour la campagne électorale et/ou libérés pour l'occasion seront mis à la disposition des Organisations Syndicales ayant déposé des listes de candidats le **lundi 23 octobre 2023** dans chaque site où des électeurs travaillent.

Par exception, sur les petits sites de moins de 30 salariés, la propagande syndicale devra être disponible dans les lutins ou des classeurs mis à disposition des salariés.

Les panneaux seront de dimensions égales et tous disposés à hauteur de vue et ne pourront pas être implantés en des lieux différents en fonction des Organisations Syndicales. L'affichage doit néanmoins avoir lieu hors de la vue du public.

L'ordre des panneaux sera déterminé par un tirage au sort réalisé en présence d'huissiers de justice le **03 octobre 2023**.

Si une liste commune est déposée, elle prend la place de l'organisation syndicale de la liste qui arrive en premier dans l'ordre du tirage au sort.

Les correspondants élections travailleront en lien avec les correspondants handicap afin de s'assurer que les panneaux d'affichage sont bien accessibles aux électeurs en situation de handicap.

12.3.2 Utilisation de la messagerie professionnelle

Conformément à l'accord du 13 mai 2019 portant sur le dialogue social au sein de l'UES Orange, l'envoi des mails aux électeurs non-inscrits sur les listes de diffusion des Organisations Syndicales n'est pas autorisé. Les dispositions prévues à l'article 29 de l'accord précité s'applique pendant la campagne électorale.

12.4 Moyens de campagne

12.4.1 Enveloppe financière

La direction versera à chaque Organisation Syndicale une enveloppe financière **0,68 cts** par électeur inscrit dans chaque Établissement Distinct où elle présentera au minimum une liste de candidats aux élections CSE titulaires 1^{er} tour.

Dans le cadre du dépôt de listes communes, prévu à l'article 10.2 du présent accord, les moyens financiers seront répartis au prorata des % indiqués par les Organisations Syndicales.

Cette enveloppe est unique pour le 1^{er} tour et l'éventuel 2nd tour, et exclusivement réservée aux listes de candidats présentées par des Organisations Syndicales.

12.4.2 Crédit Temps Complémentaire (CTC)

La direction versera à chaque Organisation Syndicale une enveloppe de **100 heures** CTC par Établissement Distinct où l'Organisation Syndicale présentera au minimum une liste de candidats aux élections CSE titulaires 1^{er} tour. Pour les élections professionnelles de 2023, cette enveloppe sera calculée sur la base de [à discuter] heures CTC par établissement distinct.

Dans le cadre du dépôt de listes communes, prévu à l'article 10.2 du présent accord, les moyens CTC seront répartis au prorata des % indiqués par les Organisations Syndicales.

Les parties conviennent qu'une partie de ces jours devra être utilisée au mois d'octobre 2023 et que l'autre partie sera utilisée au mois de novembre 2023, en conciliant à la fois les exigences de la période sur le plan d'activité et les exigences électorales.

Le volume de CTC non utilisé à la fin de la période électorale ne peut en aucun cas être reporté et sera automatiquement écrêté.

Chaque Établissement Distinct suivra la consommation du volume attribuée.

Cette enveloppe est unique pour le 1^{er} tour et l'éventuel 2nd tour, et elle est exclusivement réservée aux listes de candidats présentées par des Organisations Syndicales.

12.4.3 Heures d'Information Syndicale (HIS)

La direction accordera deux Heures d'Information Syndicale (HIS) supplémentaires par membre du personnel à déposer entre le 1^{er} septembre et le 10 novembre 2023, prises l'une et l'autre sur le temps de travail, dans le respect des contraintes de services et après information préalable du service Ressources Humaines concerné.

En pratique, les salariés ont droit à :

- une HIS par mois en septembre, octobre et novembre 2023, conformément aux dispositions de l'accord du 13 mai 2019 portant sur le « dialogue social au sein de l'UES Orange », soit 3 HIS ;

- 2 HIS supplémentaires conventionnelles à utiliser entre le 1^{er} septembre et le 10 novembre 2023, conformément au présent accord ;
- soit au maximum 5 HIS sur la période du 1^{er} septembre et le 10 novembre 2023.

Chapitre 6 – Modalités pratiques du scrutin

Article 13 – Les bureaux de vote

13.1 Le bureau de vote centralisateur

Un bureau de vote centralisateur est mis en place au niveau national.

Il sera composé d'un Président et de 6 assesseurs chargés de la surveillance des opérations de vote lors du 1^{er} tour et de l'éventuel 2nd tour.

13.2 Rôle du bureau de vote centralisateur

La mission du bureau de vote centralisateur est de veiller à la bonne organisation du scrutin et à la régularité des opérations électorales :

Période précédant le vote	<ul style="list-style-type: none">- vérifier les listes électorales, des listes de candidats et du scrutin présents dans le système de vote ;- procéder au scellement des urnes électroniques avant le début de la période de vote conformément à l'article 14.4.3;- surveiller les opérations sur le système de vote via la fonctionnalité <i>Table d'audit</i>.
Pendant la période de vote	<ul style="list-style-type: none">- contrôler et annoncer l'heure d'ouverture du vote ;- suivre le vote, via la consultation de la participation au scrutin- conserver les outils de déverrouillage du système selon la procédure décrite à l'article 14.4.3;- gérer les dysfonctionnements / périodes d'indisponibilité du site de vote qui lui seront remontés et prendre décisions afférentes éventuelles comme la suspension du vote, la prolongation de la période de vote, le déverrouillage du système de vote ou l'arrêt du scrutin en cas de stricte nécessité ;- surveiller l'intégrité du système de vote via la fonctionnalité correspondante disponible au sein du système de vote ;- surveiller les opérations sur le système de vote via la fonctionnalité <i>Table d'audit</i>. <p>En cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données, le bureau de vote a compétence, après avis des représentants susmentionnés, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote.</p>
A l'issue du vote	<ul style="list-style-type: none">- contrôler et annoncer l'heure de clôture du vote ;- surveiller les opérations sur le système de vote via la fonctionnalité <i>Table d'audit</i> et consigner tous les incidents ayant pu intervenir en cours de scrutin ;

	- éditer, vérifier et signer des procès-verbaux pour l'urne salariés de droit privé.
--	--

13.3 Les Bureaux de vote dits d' « Établissements Distincts »

Un bureau de vote unique sera constitué au sein de chaque Établissement Distinct, tels que défini par l'avenant n°3 à l'accord portant sur le dialogue social du 13 mai 2019.

pour l'ensemble des votes électroniques du scrutin CSE du périmètre de cet Établissement.

Chaque bureau de vote Établissement Distinct sera composé d'un Président et de 2 assesseurs qui auront le pouvoir de réaliser les opérations liées au déroulement et au dépouillement du vote électronique, ce pour l'ensemble des collèges CSE du périmètre de cet Etablissement.

Ces bureaux auront ainsi pour missions et responsabilités :

- le suivi du vote sur son périmètre, via la consultation de la participation au scrutin le concernant ;
- la gestion des dysfonctionnements / périodes d'indisponibilité du site de vote qui lui seront remontés, en lien avec le bureau de vote centralisateur visé à l'article 14.1 du présent accord ;
- le déclenchement du dépouillement pour les urnes CSE via le mot de passe personnel du compte utilisateur au site de supervision du Président du bureau de vote ;
- l'édition, la vérification et la signature des procès-verbaux CERFA ;
- la proclamation des résultats et l'autorisation de les diffuser ;
- l'annonce de la clôture des opérations électorales pour le scrutin CSE de son périmètre.

13.4 Règles de désignation des membres des bureaux de vote

Les Organisations Syndicales adresseront une note d'information sur l'identité de ces assesseurs :

- **lundi 30 octobre 2023 avant 12 heures** (heure de Paris) en vue du 1^{er} tour ;
- **mardi 21 novembre 2023 avant 12 heures** (heure de Paris) en cas d'éventuel 2nd tour.

Cette note devra être adressée à la Direction des Ressources Humaines du périmètre concerné pour les bureaux de vote d'Établissement Distinct et à la Direction des Relations Sociales Groupe pour le bureau de vote centralisateur.

Tout bureau de vote sera présidé, en principe, par son membre le plus âgé.

En cas de pluralité de volontaires, le principe retenu est que la présidence étant confiée au plus âgée, le premier assesseur sera celui qui vient immédiatement après le Président en âge et, le cas échéant, le second assesseur sera le plus jeune.

48 heures avant le scrutin, si la direction n'a pas reçu des Organisations Syndicales concernées la liste des assesseurs de chaque bureau de vote, elle procédera à la désignation des assesseurs manquants.

Les Organisations Syndicales veilleront également à un certain pluralisme dans la composition des bureaux de vote, étant entendu que la règle énoncée ci-dessus est en tout état de cause impérative.

Un représentant de l'employeur pourra assister aux opérations électorales en respectant une stricte neutralité et sans y prendre part.

Un délégué de liste ou, en cas d'absence, son suppléant, c'est-à-dire une personne dûment mandatée par son Organisation Syndicale qui n'appartient pas obligatoirement au bureau de vote, pourra être désigné par chaque Organisation Syndicale ayant présenté une liste de candidats dans chaque bureau de vote, pour superviser sans y participer le bon déroulement des opérations électorales au nom de son Organisation Syndicale.

Un candidat pourra être délégué de liste et/ou membre d'un bureau de vote.

Pour toute personne participant aux opérations de vote, les signes distinctifs sont interdits conformément à la législation en vigueur.

L'ensemble des membres des bureaux de vote et délégués de liste doivent faire partie du personnel de l'entreprise et le temps consacré à ces opérations sera rémunéré comme du temps de travail effectif.

Les membres des bureaux de vote recevront, avant la tenue des scrutins, une formation à leurs missions.

Article 14 – Modalités spécifiques de l'élection par voie électronique

14.1 Principes généraux

Conformément à la décision unilatérale du 16 mars 2023, les élections des représentants du personnel au CSE se dérouleront exclusivement par voie électronique

Le système de vote par voie électronique pour ces élections sera mis en œuvre par le prestataire de vote électronique et présenté aux Organisations Syndicales.

Il devra reposer sur les principes généraux du droit électoral indispensables à la régularité du scrutin et en particulier :

- intégrité du vote : identité entre le vote émis par le salarié et le vote enregistré ;
- anonymat, sincérité du vote : impossibilité de relier un vote émis à un électeur ;
- unicité du vote : impossibilité de voter plusieurs fois pour un même scrutin ;
- confidentialité, secret du vote : faculté pour l'électeur de voter pour le candidat de son choix sans pression extérieure. Cette disposition ne fait pas obstacle à la possibilité d'encourager à voter, dès lors que la liberté du choix de vote est préservée.
- accessibilité du vote : modalités de vote identiques pour l'ensemble du corps électoral.

Le cahier des charges des exigences techniques figure en annexe 5.

14.2 Protection des données personnelles

Les traitements des données personnelles opérés dans le cadre des opérations électorales font l'objet d'une documentation interne d'Orange et d'une information auprès des personnes concernées conformément à la réglementation applicable en matière de protection des données personnelles.

L'ensemble des parties prenantes aux élections respecte les principes de confidentialité et d'utilisation des données dans le strict respect de la finalité des traitements décrits ci-dessus.

Pour les seules nécessités des opérations électorales (notamment l'établissement des listes électorales), l'entreprise transmet au prestataire des fichiers établis à partir d'extraction des fichiers de gestion du personnel de l'entreprise.

Le prestataire ne traite les données que sur instruction d'Orange et dans le respect de la réglementation applicable en matière de protection des données personnelles.

14.3 Le scrutin électronique

14.3.1 Période du scrutin

Conformément à l'accord portant sur la date des élections CSE 2023 au sein de l'UES Orange du 4 avril 2023, le scrutin par voie électronique aura lieu :

- pour le 1^{er} tour : du **lundi 13 novembre 2023 à 14 heures**, heure de Paris, **au jeudi 16 novembre 2023 à 17 heures**, heure de Paris ;
- pour l'éventuel 2nd tour : **du lundi 27 novembre 2023 à 14 heures**, heure de Paris, **au mercredi 29 novembre 2023 à 17 heures**, heure de Paris.

Toute indisponibilité du site de vote au cours des scrutins pourra donner lieu, sur décision des membres du bureau de vote centralisateur national, à la prolongation du scrutin et de l'assistance téléphonique pour une durée au maximum équivalente à celle de l'indisponibilité dûment constatée.

De la même manière, le bureau de vote centralisateur national pourra prendre toute mesure d'information et de sauvegarde telle que la suspension des opérations de vote en cas de dysfonctionnement informatique ou d'attaque du système par un tiers, de défaillance technique ou d'altération des données.

14.3.2 Le site de vote

Le vote s'effectuera sur le site sécurisé dédié aux élections CSE 2023 de l'UES mis en place par le prestataire.

14.3.3 Les lieux du scrutin

Le salarié pourra voter depuis le lieu de son choix.

Le vote par voie électronique pourra s'effectuer à n'importe quel moment pendant la période de vote telle que définie à l'article 14.1.

L'employeur s'engage à garantir la mise en œuvre des conditions nécessaires permettant à tout électeur de voter en toute confidentialité sur son lieu de travail pendant la totalité de la période de vote.

14.4 Sécurisation du vote électronique

14.4.1 Validation des écrans pour les bulletins de vote électronique

Le prestataire de vote électronique assurera la programmation des pages web et notamment la présentation à l'écran des bulletins de vote.

Les logos des différentes Organisations Syndicales apparaîtront dans l'ordre tel que défini par le tirage au sort qui aura lieu le [date à définir] et qui vaudra également pour les panneaux d'affichage. A cet effet, les logos des différentes Organisations Syndicales devront être transmis à la Direction des Relations Sociales Groupe au plus tard le **lundi 9 octobre 2023**.

Le prestataire reproduira les listes de candidats telles qu'elles auront été déposées par les Organisations Syndicales.

Par ailleurs, le prestataire veillera à ce que la dimension des bulletins, les caractères et la police utilisés soient d'un type uniforme pour toutes les listes.

Les différents écrans de vote avant la validation finale seront présentés aux Organisations Syndicales nationalement et localement.

14.4.2 Matériel de vote électronique

Pour se connecter au site de vote, l'électeur devra renseigner :

- **son identifiant personnel**, reçu par courrier, conformément à la procédure décrite à l'article 2.1.5.
- **son mot de passe** : qu'il recevra (soit par mail, soit SMS, soit par message vocal) en suivant la procédure sécurisée prévue sur le site de vote.

En cas de perte de son identifiant de vote et/ou de son mot de passe, l'électeur pourra à tout moment demander sur l'espace sécurisé du site de vote la réexpédition par e-mail ou SMS d'un nouvel identifiant lui permettant de créer un nouveau mot de passe.

En parallèle, un e-mail sera envoyé sur l'adresse e-mail enregistrée dans les données électeurs pour indiquer qu'une demande de nouvel identifiant a été effectuée sur le site.

Toute indisponibilité du site de vote qui serait constatée au cours de ces périodes devra être remontée par tous moyens aux bureaux de vote, qui décideront de l'éventuelle prolongation de la durée du scrutin pour une durée maximum équivalente à celle de l'indisponibilité. L'entreprise en informera les électeurs concernés.

14.4.3 Scellement des urnes électroniques

Le scellement des urnes électroniques sera réalisé au niveau national par le bureau de vote centralisateur, en présence du prestataire et des délégués de liste :

- pour le 1^{er} tour : le **vendredi 10 novembre 2023 à 10 heures** (Heure de Paris) dans les locaux de la Direction ;
- pour l'éventuel 2nd tour : le **vendredi 24 novembre 2023 à 10 heures** (Heure de Paris) dans les locaux de la Direction.

La première étape consiste à vérifier les listes électorales, les listes de candidats et les éléments du scrutin

La vérification préalable prendra la forme d'une recherche par échantillonnage, c'est-à-dire qu'il sera recherché :

- pour ce qui concerne les électeurs : d'une part, au minimum 3 noms de personnes ayant la qualité d'électeurs seront donnés par le bureau de vote centralisateur pour vérifier qu'ils apparaissent bien dans le système ; d'autre part, au minimum 3 noms de personnes n'ayant pas la qualité d'électeur seront donnés par le Bureau de vote centralisateur pour vérifier qu'ils n'apparaissent pas dans le système ;
- pour ce qui concerne les candidats, 1 liste de candidats sur l'ensemble de l'élection sera donnée par chaque organisation syndicale : non seulement de sa place dans l'ordre des listes pour le scrutin envisagé (vérification de sa conformité par rapport au tirage au sort) ; mais encore de ce que le logo, la profession de foi ainsi que l'ordre des candidats, soient conformes aux éléments transmis ;
- pour ce qui concerne les données relatives aux scrutins (dates, heures, répartition des sièges entre les collèges), 1 scrutin d'un périmètre CSE sera donné par organisation syndicale avec au moins 3 périmètres test.

Une fois la validation globale des données présentes dans le système opérée, il ne sera plus possible de les modifier.

Cette validation permet de générer des phrases secrètes pour le scellement des urnes électroniques.

La deuxième étape consiste à générer les phrases secrètes.

Il est convenu que 3 personnes, membres du bureau de vote centralisateur, détiendront chacune une phrase secrète pour l'ensemble des urnes électroniques et que le déverrouillage sera réalisé par le renseignement de 2 phrases secrètes dans le système. Le nom de ces 3 personnes sera renseigné dans le système par le prestataire.

Chaque détenteur d'une phrase secrète choisira, à tour de rôle, un mot de passe qu'il renseignera dans le système.

Afin de prévenir un oubli de ce mot de passe entre le moment où son détenteur le crée et le moment du dépouillement, il est prévu que chaque détenteur inscrive de manière manuscrite son mot de passe sur un bulletin papier qui sera inséré dans une enveloppe : ces 3 enveloppes, conservées par des huissiers, ne seraient ouvertes qu'au moment du dépouillement par leurs détenteurs s'ils avaient oublié une phrase secrète. En cas d'organisation de la cérémonie de scellement à distance, chaque détenteur est chargé de conserver son mot de passe.

La troisième étape est le vote à blanc.

Avant le scellement, un test ou vote « à blanc » sera alors réalisé, afin de vérifier la fiabilité et l'intégrité du système en présence des représentants des listes de candidats et de la cellule d'assistance technique du prestataire.

Ainsi, les actions suivantes seront effectuées avant que le vote ne soit ouvert :

- un test du système de vote électronique vérifie que l'urne électronique est vide, scellée et chiffrée par les phrases secrètes ;
- avant que le vote ne soit ouvert, un test spécifique du système de dépouillement à l'issue duquel le système est scellé.

La quatrième et dernière étape est le scellement des urnes.

Une fois ce vote à blanc réalisé, les urnes seront vidées et il sera procédé au scellement définitif des urnes, lequel fera l'objet d'un procès-verbal, édité à partir du poste du prestataire.

Les enveloppes contenant les mots de passe seront remises par leur détenteur à des huissiers de justice qui les conserveront jusqu'au dépouillement.

Le scellement des urnes sera régulièrement contrôlé pendant la durée du scrutin.

14.5 Déroulement du vote électronique : le parcours électeur [à valider avec prestataire]

14.5.1 Etape 1 : connexion au site de vote et authentification

Les électeurs auront la possibilité de voter en toute confidentialité et à tout moment pendant la durée du scrutin, à partir de n'importe quel terminal disposant d'une connexion internet, sur leur lieu de travail, à partir de leur domicile ou de tout autre lieu.

L'électeur se connecte au site de vote grâce à l'URL qui lui a été communiqué par courrier, push mail et intranet. Les différentes communications (hors courriers) proposeront un lien renvoyant directement au site de vote.

Une fois connecté au site de vote, il s'authentifie en renseignant son identifiant et mot de passe personnel définis à l'article 14.4.2.

14.5.2 Etape 2 : Choix du vote

Après s'être ainsi connecté et authentifié sur le site de vote, le service affichera les élections auxquelles l'électeur est autorisé à participer.

L'électeur devra sélectionner le scrutin pour lequel il souhaite voter. Les élections pour lesquelles il aurait déjà voté ne seront plus sélectionnables.

Sur l'écran suivant, l'électeur devra ensuite saisir son vote en cochant la liste de candidats de son choix ou, s'il le souhaite, la case « Je vote blanc ».

En cochant une liste, l'électeur aura la possibilité, s'il le souhaite, de rayer un ou plusieurs noms de candidats de cette liste : il lui suffira pour ce faire de décocher les noms qu'il souhaite rayer.

Un « pop-up » d'alerte apparaîtra à l'écran afin d'indiquer à l'électeur qu'il s'apprête à rayer un ou plusieurs noms.

Le panachage de listes n'étant pas permis, le site ne permettra pas de cocher plusieurs listes et/ou le cas « Je vote blanc ».

Il a la possibilité de consulter les professions de foi attachées à chaque liste de candidats avant de voter

14.5.3 Etape 3 : Validation du vote

Tant que l'électeur n'aura pas validé son vote, il pourra le modifier.

La validation de chaque vote vaudra signature par l'électeur de la liste d'émargement : cette confirmation finale du vote sera donc définitive et générera un accusé de réception qui sera envoyé par e-mail à l'électeur. Il pourra également le consulter à l'écran, ou le télécharger au format PDF pour le sauvegarder et/ou l'imprimer.

L'électeur pourra ensuite se déconnecter du système.

En tout état de cause, si à l'heure de clôture du scrutin, un électeur est toujours connecté, il sera automatiquement déconnecté du système. Si à cette même-heure, il n'avait pas validé son vote, ce dernier ne pourrait pas être pris en compte.

Par ailleurs, en cas d'inaction de l'électeur pendant au moins 10 minutes, il sera automatiquement déconnecté du système de vote.

L'authentification par les codes d'accès permet de garantir l'unicité du vote réalisé par l'électeur titulaire de ces codes : personne ne pourra plus voter une nouvelle fois avec ces mêmes codes d'accès.

14.6 Données consultables pendant le scrutin

La liste d'émargement sera accessible depuis le site de supervision aux membres des bureaux de vote (Centralisateur/ Établissement Distinct) et aux délégués de liste à des fins de contrôle de

déroulement du scrutin. Dès la clôture du scrutin, les listes d'émargement seront figées, horodatées et scellées automatiquement sur l'ensemble des serveurs.

Pendant le scrutin, la direction enverra aux organisations syndicales les listes d'émargement, 1 fois par demi-journée, au format PDF.

Le taux de participation au scrutin sera accessible, pendant la durée des scrutins, par les membres des bureaux de vote ainsi que les délégués de chaque liste qui auront été désignés par les organisations syndicales au niveau central et au niveau Établissement distinct.

Aucun résultat partiel ne sera disponible pendant la durée des scrutins.

Article 15 - Les bulletins de vote

Les bulletins de vote électroniques porteront très lisiblement les mentions suivantes :

- « Élections CSE » ;
- la date et le tour ;
- l'indication du collège ;
- «Titulaires» ou «Suppléants» ;
- le sigle ou le logo de l'Organisation Syndicale ainsi que le cas échéant un slogan court. Dans l'hypothèse d'une liste commune, les organisations syndicales fourniront un sigle ou un logo commun ainsi que le cas échéant, un slogan court. Pour le 2nd tour éventuel, la mention « liste sans étiquette » ou la mention de l'Organisation Syndicale, les noms et prénoms des candidats et leur entité de rattachement.

Article 16 - Assistance Hotline

L'électeur qui aura besoin d'éclairages sur le vote électronique ou de faire connaître un dysfonctionnement dans le déroulement des élections (erreur sur ses coordonnées en tant qu'électeur, indisponibilité du site de vote pendant la période de vote...) pourra utilement contacter le numéro qu'il trouvera sur dans chacune des communications, où une personne enregistrera la demande et apportera toutes les réponses nécessaires dans les meilleurs délais.

La hotline est l'unique point d'entrée pour les demandes, de la part des électeurs, de correction des listes électorales. Les demandes de modification de listes électorales doivent être adressées auprès de cette assistance téléphonique avant **le vendredi 13 octobre 2023 à 12 heures (heure de Paris)**.

Cette hotline sera joignable dès **le lundi 9 octobre**. Une assistance complémentaire par mail sera mise en place pour les salariés situés en dehors de la France hexagonale.

A l'issue du scrutin, le prestataire est en mesure de fournir le journal complet des appels, le motif de chaque appel ainsi qu'un compte rendu précis des actions menées dans le cadre de sa prestation d'assistance téléphonique. Les actions de l'assistance sont vérifiables à tout moment en cours d'opération et a posteriori.

Article 17 – Dépouillement

17.1 Contrôles préalables et descellement des urnes électroniques

Le bureau de vote Établissement Distinct annonce publiquement la fermeture du scrutin.

Avant donner l'autorisation du dépouillement aux bureaux de vote Établissement Distinct à, le bureau de vote centralisateur défini dans l'article 13.1 du présent accord :

- contrôlera que les scrutins seront tous clos et que les urnes seront toujours scellées dans le système de vote ;
- puis procédera publiquement au déverrouillage des urnes, par l'introduction successive dans l'ordinateur du prestataire, de 2 des 3 phrases secrètes dans les conditions expliquées à l'article 14.3 du présent accord

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.

17.2 Déroulement du dépouillement

Le dépouillement des votes s'effectuera par les membres de chaque bureau de vote d'Établissement Distinct. Pour effectuer le dépouillement, un membre de chaque bureau de vote saisira le mot de passe de son compte utilisateur du site de supervision.

En cas de perte de l'un de ces codes, le bureau de vote pourra demander à s'en voir réattribuer un nouveau via le site de supervision.

Le dépouillement sera réalisé par chaque bureau de vote tels que définis dans l'article 13.2 du présent accord en présence d'un représentant de l'employeur, ainsi que des délégués de liste s'ils le souhaitent.

Il est rappelé que les électeurs ont le droit de raturer le nom d'un candidat sur la liste pour laquelle ils votent, toutefois ces ratures sont prises en considération uniquement si elles atteignent ou dépassent 10 % des suffrages valablement exprimés pour la liste. Dans le cas contraire, les candidats sont déclarés élus, compte tenu du nombre de voix obtenues par la liste, dans l'ordre de leur présentation sur la liste.

Cette règle ne s'applique pas au calcul de la plus forte moyenne. En effet, celle-ci se détermine en déduisant les noms raturés du total des voix de la liste même si le pourcentage de ratures est inférieur à 10 %.

Au 1^{er} tour, une fois le décompte des suffrages valablement exprimés fait, le bureau de vote vérifie si le quorum est atteint. La vérification de l'atteinte ou non du quorum ne peut se faire qu'après dépouillement, puisque le quorum n'est atteint que si les suffrages valablement exprimés (votants moins les votes blancs et nuls) représentent au moins la moitié des inscrits. Le quorum s'apprécie pour chaque vote, c'est-à-dire dans chaque collège, et à l'intérieur de chaque collège, pour les titulaires et pour les suppléants.

Le nombre des suffrages valablement exprimés sera égal au nombre de votants diminué de celui des bulletins blancs.

Article 18 – Proclamation et publicité des résultats

Au terme du dépouillement, la clôture des opérations électorales se solde par la proclamation des résultats par le Président du bureau de vote et par l'édition du procès-verbal correspondant.

18.1 Procès-verbaux CERFA

Les PV seront vérifiés puis signés par le bureau de vote Établissement Distinct. Le président de chaque bureau de vote doit constater publiquement les heures d'ouverture et de clôture du scrutin et les mentionner au procès-verbal. Le PV porte inscription de toutes observations, protestations ou contestations sur les opérations électorales.

Les PV doivent être paraphés et signés par les membres du bureau de vote, les noms, prénoms, et le cas échéant, l'Organisation syndicale des membres doit être renseignée.

Ils seront adressés par les directions concernées en double exemplaire à l'inspection du travail compétente.

Une copie électronique de ces PV sera en outre transmise aux Organisations Syndicales ayant présenté des candidats à l'élection concernée par ces PV. Une copie électronique sera également remise aux autres Organisations Syndicales de l'entreprise ayant participé à la négociation d'au moins un Protocole d'Accord Préélectoral dans le cadre de ces élections le plus rapidement possible. Il est rappelé que seuls les membres des bureaux de vote sont autorisés à porter des inscriptions sur les PV.

Une annexe spécifique au PV devra attester de la vérification des listes d'émargement.

18.2 Proclamation des résultats

Chaque bureau de vote proclamera le résultat de chaque scrutin "Titulaires" et "Suppléants". Au cours de cette proclamation, il sera procédé à l'énoncé :

- du nombre d'inscrits du collège considéré ;
- de celui des votants ;
- de celui des suffrages valablement exprimés ;
- du nombre de sièges revenant à chaque liste ;
- des noms des élus et du nombre de voix obtenues par chacun d'eux.

En présence d'un système de vote électronique, les résultats seront accessibles sur le site de vote et généreront les PV CERFA correspondants au format PDF.

18.3 Affichage des résultats

Les résultats seront affichés dans chaque Établissement Distinct pour le scrutin CSE pour communication au personnel.

Ces résultats seront accessibles sur le site de vote.

18.4 Transmission des résultats concernant les salariés de droit privé au Ministère du travail (MARS)

Pour le premier tour des élections CSE titulaires uniquement, il sera distingué au sein d'urnes séparées les votes « salarié de droit privé » ou « fonctionnaire » en vue de disposer de l'ensemble des éléments nécessaires à la branche des télécoms pour apprécier la représentativité à ce niveau.

Le PV des résultats du scrutin des salariés de droit privé aux élections professionnelles CSE de l'UES Orange sera signé par les membres du bureau de vote centralisateur.

Il est rappelé qu'à aucun moment les résultats du scrutin servant à déterminer la représentativité des Organisations Syndicales au niveau de l'UES n'opéreront cette distinction.

18.5 Attribution des sièges

Chaque bureau de vote procède à l'attribution des sièges pour chaque collège et pour chaque catégorie (titulaires/suppléants) dans lequel le quorum est atteint en calculant le quotient électoral de chaque collège : nombre total de suffrages valablement exprimés dans le collège / nombre de sièges à pourvoir dans ce collège.

Ce quotient est le même pour chaque liste.

Il est attribué à chaque liste autant de sièges que le nombre de voix recueillies par elle contient de fois le quotient électoral.

Pour ce faire, la moyenne de chaque liste est calculée pour chaque scrutin : addition du nombre de voix obtenues par chaque candidat de la liste divisée par le nombre de candidats sur la liste.

Le bureau de vote attribue ensuite à chaque liste le nombre de sièges égal à sa moyenne de liste divisée par le quotient électoral.

Les sièges restants sont attribués à la plus forte moyenne.

En cas de parfaite égalité, le siège est attribué à la liste qui a le plus grand nombre de voix. Si deux listes ont recueilli le même nombre de voix, le siège est attribué au candidat le plus âgé susceptible d'être élu.

18.6 Communication des résultats détaillés aux Organisations Syndicales

Les résultats des élections CSE seront disponibles à la maille Établissement Distinct.

Chapitre 7 – Dispositions finales

Article 19 – Durée de l'accord

Le présent accord entrera en vigueur le jour qui suit les formalités de dépôt auprès des services compétents, conformément aux articles L. 2231-6 et D. 2231-2 du code du travail.

Il est conclu pour la mise en œuvre du scrutin CSE 2023, dont les dates sont les suivantes :

- **du 13 au 16 novembre 2023 pour le 1er tour ;**
- **du 27 au 29 novembre 2023 pour l'éventuel 2nd tour.**

Article 20 – Modalités de révision

Une procédure de révision pourra être engagée avant le déroulement des élections professionnelles, dans les conditions fixées aux articles L. 2261-7 et suivants du code du travail.

La demande de révision devra être portée à la connaissance des autres signataires par lettre recommandée avec accusé de réception, et devra être accompagnée d'un projet sur le ou les articles concernés.

Les négociations commenceront le plus rapidement possible avec l'ensemble des Organisations Syndicales Intéressées dans le champ d'application du présent accord et habilitées, au terme de l'article L. 2261-7-1 du code du travail précité, à engager cette procédure de révision.

Article 21 – Notification et formalités de dépôt

En application de l'article L. 2231-5 du code du travail, la partie la plus diligente des organisations signataires notifie le texte à l'ensemble des Organisations Syndicales Intéressées à l'issue de la procédure de signature.

Les formalités de dépôt et de publicité seront par ailleurs réalisées dans les conditions fixées aux articles D. 2231-2, D. 2231-4 et L. 2231-5-1 du code du travail :

- un exemplaire du présent accord sera déposé au greffe du Conseil des Prud'hommes du lieu de conclusion du protocole ;
- le présent accord et les pièces accompagnant le dépôt prévues aux articles D. 2231-6 et D. 2231-7 du code du travail seront déposés sur la plateforme de télé-procédure du ministère du travail. Conformément à l'article L. 2231-5-1 du code du travail, ce protocole sera publié en ligne dans un standard ouvert aisément réutilisable. La version déposée ne comportera pas les noms et prénoms des personnes signataires.

Les éventuels avenants de révision du présent accord feront l'objet des mêmes mesures de dépôt et publicité.

Fait à Issy-les-Moulineaux, le 3 juillet 2023

La Direction pour les sociétés composant l'UES Orange

Eric Bousquet

Directeur des Relations Sociales

Les Organisations Syndicales

Pour la CDMT :	Pour la CFDT-F3C :	CFDT-PT :
Pour la CFE-CGC ORANGE :	Pour la CFTC :	Pour la CGT-FAPT :
Pour la CGTG :	Pour la CGTR :	Pour la CGTM-P&T :
Pour la CTU :	Pour FOCom :	Pour Orange Ensemble :
Pour Printemps Ecologique :	Pour le SNE :	Pour le STC :
Pour SUD-PTT :	Pour l'UNSA :	Pour l'UTG :

Pour l'UTT UGTG :	Pour l'UTG M :
-------------------	----------------

La signature numérique emporte votre consentement sur l'ensemble du document. Elle rend inutile le paraphe de chaque feuille. La date de signature du document figure sur la signature numérique.

Pour être valable, un document doit être signé numériquement par tous les signataires.

Si ce document venait à être signé de manière manuscrite, la version numérique serait caduque et non opposable. Le document papier devra alors être paraphé, daté et signé.

Réserves Printemps Ecologique

Printemps Ecologique considère que l'impossibilité d'utiliser à titre exceptionnel, dans le cadre de l'élection, les moyens de communication numérique de manière globale afin de permettre aux organisations syndicales de pouvoir recueillir directement les consentements dans le respect des droits fondamentaux en matière de protection des données, pourrait constituer une rupture d'égalité électorale.

Annexe n°1 - Détermination du nombre de sièges par établissements distinct (CSEE), et répartition des sièges entre les collèges

Etablissement Distinct	TOTAL eff ETP int./ext.	TOTAL sièges	Collège 1		Collège 2		Collège 3	
			ETP	Sièges	ETP	Sièges	ETP	Sièges
Direction Technique et Système d'Information (DTSI)	14 089,63	40	66,62	1	2249,27	6	11773,74	33
Direction Orange Ile de France (DO IDF)	8 484,75	37	890,13	4	3643,78	16	3950,84	17
Direction Orange Grand Sud Ouest (DO GSO)	7 749,52	35	1196,63	5	3891,97	18	2660,92	12
Direction Orange Grand Sud Est (DO GSE)	7 528,81	35	1029,45	5	3752,03	17	2747,33	13
Direction Orange Grand Nord Est (DO GNE)	7 053,92	35	1030,45	5	3515,34	17	2508,13	13
Direction Orange Grand Ouest (DO GO)	6 899,29	34	989,88	5	3342,13	16	2567,28	13
Services Communications Entreprises (SCE)	5 938,94	32	22,64	1	542,40	3	5373,90	28
Fonctions Corporate (FC)	4 955,10	30	79,86	1	540,43	3	4334,81	26
Orange Innovation (INNOV)	4 292,27	29	15,25	1	36,81	1	4240,21	27
Orange France Siège (OFS)	3 676,08	28	8,03	1	87,04	1	3581,01	26
Orange Wholesale (OW)	2 681,22	25	27,36	1	479,35	4	2174,51	20
Antilles-Guyane (AG)	1 454,27	23	188,55	3	444,08	7	821,65	13
Direction Orange Réunion Mayotte (DO RM)	1 007,63	19	101,02	2	369,71	7	536,91	10
Direction Régionale Renforcée Corse (DRR C)	442,49	13	118,01	4	183,70	5	140,78	4
TOTEM France	121,93	6			17,85	1	104,08	5
TOTAL	76 375,85	421	5 763,87	39	23095,88	122	47516,10	260

Annexe n°2 - Répartition des sièges du CSEC

Etablissement Distinct	ETP au 31 janvier 2023	Nombre élus titulaires CSEC Total	Nombre élus suppléants CSEC Total
Direction Technique et Système d'Information (DTSI)	14 089,63	2	3
Direction Orange Ile de France (DO IDF)	8 484,75	2	2
Direction Orange Grand Sud Ouest (DO GSO)	7 749,52	2	2
Direction Orange Grand Sud Est (DO GSE)	7 528,81	2	2
Direction Orange Grand Nord Est (DO GNE)	7 053,92	2	2
Direction Orange Grand Ouest (DO GO)	6 899,29	2	2
Services Communications Entreprises (SCE)	5 938,94	2	2
Fonctions Corporate (FC)	4 955,10	2	2
Orange Innovation (INNOV)	4 292,27	2	2
Orange France Siège (OFS)	3 676,08	2	2
Orange Wholesale (OW)	2 681,22	1	2
Antilles-Guyane (AG)	1 454,27	1	2
Direction Orange Réunion Mayotte (DO RM)	1 007,63	1	0
Direction Régionale Renforcée Corse (DRR C)	442,49	1	0
TOTEM France	121,93	1	0
TOTAL	76 375,85	25	25

Annexe n°3 - Planning du 1^{er} tour du scrutin CSE du 13 au 16 novembre 2023

Tous les horaires affichés s'entendent **en heure de Paris** sauf exception signalée par *

Dates 2023	Actions
A partir de la semaine du 25 septembre	Envoi postal de la lettre d'information annonce des élections/extrait liste électorale /et/ou la communication électorale (art 11.2)
Jeudi 03 octobre	Tirage au sort au niveau national de l'ordre des panneaux d'affichage (art 12.3.1)
Lundi 9 octobre 2023	Envoi des logos à DRSG par les OS (art 12.2)
Mardi 10 octobre 2023	Annonce des élections au personnel par voie d'affichage (art 11.2)
Mardi 10 octobre 2023 14H00*	Affichage des listes électorales provisoires (art 8.1.1) Ouverture de la hotline (art 16) Ouverture de l'espace de communication (art.11.1.3)
Vendredi 13 octobre 2023 12H00	Fin du délai de réclamation des listes électorales provisoires (art 8.1.1)
Mardi 17 octobre 2023 14H00*	Affichage des listes électorales rectifiées (art 8.1.2)
Vendredi 20 octobre 2023	Fin du délai de recours en justice pour les électeurs devant les tribunaux (art 8.1.2)
Lundi 23 octobre 2023 avant 12H00*	Dépôt des candidatures/listes de candidats des OS (art 10.2) Date limite de remise par les OS à DRSG des professions de foi nationale et locales sous format électronique (art.12.1) Mise à disposition des panneaux d'affichage syndicaux
Lundi 23 octobre 2023 14H00*	Affichage éventuel des listes électorales définitives (en cas de modification suite à un recours judiciaire) (art 8.1.3)

Dates 2023	Actions
Du 23 octobre au 27 octobre 2023	Validation des listes de candidats au niveau local
Lundi 30 octobre 2023	Liste des assesseurs (art. 13.4)
Mardi 31 octobre 2023 14H00*	Affichage des listes de candidats (art 10.3) Envoi push mail aux salariés (art. 11.4)
Semaine du 6 novembre 2023	Envoi postal du matériel de vote électronique 1 ^{er} tour (art. 11.3)
2 novembre et 10 novembre 2023	Envoi par la Direction des <i>push mail</i> relatifs aux tracts syndicaux à l'ensemble des salariés (art 12.1)
Vendredi 10 novembre 2023	Cérémonie de scellement <ul style="list-style-type: none"> ▪ création et validation des membres du bureau de vote ; ▪ génération et attribution des phrases secrètes ; ▪ réalisation du vote à blanc ; ▪ scellement du système (article 14.4.3).
Lundi 13 novembre 2023	(à 14h00 heure de Paris) Ouverture de la période de vote électronique 1 ^{er} tour (entre 14h00 et 16h00 heure de Paris) Envoi du mail d'annonce d'ouverture du site vote pour le 1 ^{er} tour

Dates 2023	Actions
<p align="center">Jeudi 16 novembre 2023</p>	<p><u>à 17h00 (heure de Paris)</u> Fin de la période de vote électronique 1^{er} tour</p> <p><u>à partir de 17h00 (heure de Paris) :</u></p> <ul style="list-style-type: none"> ▪ descellement du système de vote en centralisé ▪ clôture du scrutin ▪ saisie du code de dépouillement par le Président du bureau de vote ▪ dépouillement ▪ attribution des sièges (si quorum atteint) ▪ établissement et signature des PV CERFA ▪ diffusion des résultats du 1^{er} tour aux établissements distincts et aux OS ▪ affichage des résultats du 1^{er} tour

Annexe n° 4 - Planning du 2nd tour éventuel du scrutin CSE du 27 au 29 novembre 2023

En cas de carence au 1^{er} tour ou si le quorum n'a pas été atteint ou si tous les sièges n'ont pas été pourvus, un 2nd tour sera organisé.

Tous les horaires affichés s'entendent en heure de Paris sauf exception signalée par *

Dates 2023	Actions
Mardi 21 novembre 2023 avant 12H00	Date limite de dépôt des candidatures, syndicales ou libres (art.10.2) Date limite de dépôt des professions de foi (art 12.1)
Mardi 21 novembre 2023 avant 12H00	Date limite pour les OS pour faire connaître à la Direction la liste des assesseurs (art.13.4)
Judi 23 novembre 2023 avant 12H00*	Affichage des listes de candidats (art 10.3)
Vendredi 24 novembre 2023	Envoi par la Direction du 2 nd <i>push mail</i> relatifs aux tracts syndicaux à l'ensemble des salariés (art.12.1)
Vendredi 24 novembre 2023 à 10H00	<ul style="list-style-type: none">▪ cérémonie de scellement▪ création et validation des membres du bureau de vote▪ génération et attribution des phrases secrètes▪ réalisation du vote à blanc▪ scellement du système (art 14.4.3)
Lundi 27 novembre 2023 à 14H00	Ouverture de la période de vote électronique 2 nd tour 14h00 (heure de Paris)

Dates 2023	Actions
<p style="text-align: center;">Mercredi 29 novembre 2023 à 17H00</p>	<p>à 17h00 (heure de Paris) Fin de la période de vote électronique 2nd tour</p> <p>à partir de 17h00 (heure de Paris) :</p> <ul style="list-style-type: none"> ▪ descellement du système de vote en centralisé ▪ clôture du scrutin ▪ saisie du code de dépouillement par le Président du bureau de vote ▪ dépouillement ▪ attribution des sièges ▪ établissement et signature des PV CERFA ▪ diffusion des résultats des élections (1^{er} et 2nd tours) aux établissements ▪ affichage des résultats des élections (1^{er} et 2nd tours)

Annexe n° 5 - Cahier des charges de mise en œuvre du vote électronique pour les élections CSE 2019

ELECTIONS CSE 2023

Cahier des charges de mise en œuvre du vote électronique

Vos contacts pour tous renseignements ou informations complémentaires

Chef de projet élections

Eric BOUSQUET –
Directeur des Relations Sociales du Groupe
Tel : 06 62 92 02 30
Mail : eric.bousquet@orange.com

Equipe projet élections

Cédric CARVALHO
Tel : 06 32 00 78 37
Mail : cedric.carvalho@orange.com

Michèle DILOUYA
Tel : 06 30 51 07 46
Mail : michele.dilouya@orange.com

Marie Juliette FRITZ (Juriste)
Tel : 07 86 50 91 57
Mail : mariejuliette.fritz@orange.com

Magalie DE FLEURY (Juriste)
Tel : 06 73 44 98 57
Mail : magalie.defleury@orange.com

Equipe technique

Marc GOUSPY
Tel : 06 37 55 67 32
Mail : marc.gouspy@orange.com

SOMMAIRE

I - Contexte de mise en œuvre du vote électronique.....	57
II- Caractéristiques des scrutins	58
III - Pilotage du projet.....	59
1/ Moyens mis en œuvre.....	59
2/ Pilotage en phase de construction/préparation.....	59
3/ Bilan de la prestation (qualitatif et quantitatif)	59
IV – Le système de vote : architecture technique	60
1/ Sécurisation du système proposé.....	60
<i>a. Principes généraux</i>	60
<i>b. Respect de la réglementation sur la protection des données personnelles</i>	61
<i>c. Fourniture d'un rapport d'expertise</i>	62
2/ Système de vote électronique distant	63
3/ Disponibilité du système de vote électronique	64
4/ Accessibilité	64
<i>a. Compatibilité des terminaux</i>	64
<i>b. Respect des normes d'accessibilité numérique</i>	65
5/ Accès aux informations sur les matériels et dans les locaux du prestataire	65
V – Préparation des élections	65
1/ Contribution du prestataire aux modalités d'organisation des élections.....	65
2/ Phase de test et de recette du système de vote électronique	66
3/ Listes électorales.....	67
<i>a. Constitution des fichiers</i>	67
<i>b. Confidentialité des fichiers</i>	67
<i>c. Mise à jour des listes électorales</i>	68
<i>d. Accès aux listes électorales sur le site de gestion de l'organisateur du scrutin</i>	68
4/ Liste de candidats.....	69
<i>a. Constitution des fichiers</i>	69
<i>b. Injection des fichiers dans le système de vote</i>	69
<i>c. Format des fichiers</i>	69
5/ Génération et envoi des informations relatives aux élections.....	70
<i>a. Courriers et push mails</i>	70
<i>b. Codes d'accès au système de vote électronique</i>	70

6/ Espace de communication	71
<i>a. Contenu de l'espace de communication</i>	71
<i>b. Accès aux listes électorales</i>	71
7/ Formation	71
VI- Le vote	72
1/ Organisation des bureaux de vote	72
2/ Scellement des urnes	72
3/ Durée du vote	73
4/ Vote électronique	73
<i>a. Chiffrement des bulletins de vote dans l'urne électronique</i>	73
<i>b. Dispositifs de secours</i>	74
<i>c. Scenario de vote</i>	74
<i>d. Enchaînement des élections</i>	75
<i>e. Emargement électronique, unicité du vote</i>	75
<i>f. Taux de participation</i>	75
5/ Assistance technique.....	75
6/ Assistance téléphonique salariés	76
VII – Dépouillement et résultats	76
1/ Dépouillement des urnes électroniques et déchiffrement des bulletins de vote	76
2/ Remise des résultats	76
3/ Données à fournir à l'issue de la consolidation des résultats	76
<i>a. Les résultats</i>	76
<i>b. Procès-verbaux des élections</i>	77
<i>c. Listes d'emargement</i>	77
VIII – Archivage, conservation et destruction des données.....	77

I - Contexte de mise en œuvre du vote électronique

Dans le cadre de l'organisation des élections pour les Comités Economiques et Sociaux (CSE), Orange souhaite mettre en place une solution de vote par voie électronique sur Internet.

La date des élections sera fixée par voie d'accord pour qu'elles aient lieu dans les 15 jours précédant la date de fin de la mandature 2019-2022, fixée au 3 décembre 2023 inclus.

Le vote électronique sera également encadré soit par un accord, soit, à défaut d'accord, par une Décision Unilatérale conformément aux articles L.2314-26 et R.2314-5 du code du travail.

Le prestataire aura en charge, sous le contrôle de la Direction des Relations Sociales du Groupe Orange :

- la conception et la mise en place du système de vote électronique conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (pour une élection avec un niveau de risque fixée à 2) ;
- la gestion de la préparation des élections par voie électronique ;
- la mise en œuvre du système de vote électronique conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (pour une élection avec un niveau de risque fixée à 2) ;
- la mise en œuvre du système de dépouillement des bulletins de vote électronique et l'élaboration des états des résultats permettant l'affectation des sièges ; conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (pour une élection avec un niveau de risque fixée à 2) ;
- la production de l'ensemble des statistiques relatives aux différentes élections.

La prestation confiée par Orange au prestataire fera l'objet d'un contrat de prestations de services entre Orange et le prestataire, conforme aux lois applicables en matière de protection des données.

Dans la mesure où le prestataire intervient en tant que sous-traitant dans la mise en œuvre d'un traitement de données personnelles, ce dernier s'engage à assurer à Orange « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (article 28 du règlement général sur la protection des données personnelles).

La prestation devra respecter la loi pour une république numérique, conformément au Décret n°2019-768 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne.

II- Caractéristiques des scrutins

Les élections à organiser sont des élections des représentants du personnel pour les Comités Economiques et Sociaux d'Etablissement (CSEE).

Base légale	Art. L2314-4 à L2314-32 du code du travail
Scrutin	Par périmètre d'Etablissement Distinct Scrutin de liste à deux tours avec représentation proportionnelle à la plus forte moyenne (Art. L2414-29)
Périmètre	Périmètre UES Orange (Orange SA, Orange Caraïbe (*) et TOTEM France) (*) (Processus de consultation en cours du projet de fusion d'Orange Caraïbes au sein d'Orange SA)
Nombre d'électeurs	Environ 75 000
Nombre de collège	2 à 3 collèges avec une possibilité de collège unique pour certains scrutins

III - Pilotage du projet

1/ Moyens mis en œuvre

Le prestataire retenu nommera au sein de sa structure **un Chef de projet dédié** à ces élections qui pilotera la prestation dans sa globalité et **qui sera présent du début à la fin du processus**. Ce chef de projet sera le correspondant unique de l'équipe projet d'Orange et sera en charge :

- de coordonner l'ensemble des acteurs et assurer la responsabilité de l'interface avec Orange ;
- de répondre en temps réel aux sollicitations de l'équipe projet Orange ;
- d'être force de propositions sur les éventuelles actions à mener tout au long du processus de vote
- de mettre à disposition les moyens humains et matériels nécessaires ;
- d'assurer la tenue du planning et la mise en place du système de vote (adaptation du contexte de l'opération, paramétrage, intégration des données...).

2/ Pilotage en phase de construction/préparation

Le prestataire devra s'assurer du bon déroulement des opérations, notamment :

- dans le respect des délais ;
- en s'assurant de la conformité du résultat par rapport aux exigences spécifiées ;
- avec toutes les garanties de sécurité et de confidentialité ;
- via la mise en place d'un processus de planification, de validation et de contrôle tout au long du projet, assurant une visibilité totale sur l'avancement des travaux et sur la qualité des livrables.

Il sera chargé de planifier une série de points de rencontre avec l'équipe projet Orange au lancement du projet et tout au long du processus, permettant de mesurer le bon déroulement de l'opération.

3/ Bilan de la prestation (qualitatif et quantitatif)

Ce bilan devra permettre d'identifier et expliquer les éventuels écarts de réalisation par rapport au présent cahier des charges, et proposer des actions correctives ou des pistes d'amélioration pour de futures élections.

Il portera sur le déroulé du scrutin ainsi que sur les phases de préparation en amont.

IV – Le système de vote : architecture technique

1/ Sécurisation du système proposé

Le système de vote électronique proposé par le prestataire devra répondre aux exigences décrites ci-après.

a. Principes généraux

Le système doit notamment :

- assurer la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges électoraux ;
- garantir la sécurisation du vote ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes ;
- permettre que les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne ne soient accessibles qu'aux personnes chargées de la gestion et de la maintenance du système ;
- garantir un chiffrement des données dès l'émission du vote sur le poste de l'électeur ;
- garantir que la liste d'émargement ne soit accessible qu'aux membres du bureau à des fins de contrôle du bon déroulement du scrutin ;
- garantir qu'aucun résultat partiel soit accessible pendant le déroulement du scrutin ;
- garantir que les données relatives aux électeurs inscrits sur les listes électorales et les données relatives au vote soient traités par des systèmes informatiques distincts, dédiés et isolés respectivement nommés fichier électeurs et contenu de l'urne électronique ;
- garantir l'enregistrement des listes d'émargement précisant la date et l'heure du vote sur un support distinct de l'urne électronique, scellée, non réinscriptible rendant son contenu inaltérable et probant ;
- être scellé à l'ouverture du scrutin afin de garantir la non altération des composants constituant la solution de vote (fichiers des électeurs, candidats, scrutins et applications) ;
- être scellé à la clôture du scrutin. 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 ;
- permettre le dépouillement que par activation d'au moins deux clefs de chiffrement différentes sur les trois qui doivent être édités ;
- prévoir un système de secours susceptible de prendre le relais en cas de panne du système principal ;
- prévoir la conservation sous scellée des fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement les fichiers de résultats et de sauvegarde jusqu'à l'expiration du délai de recours ou en cas d'action contentieuse la décision juridictionnelle devenue définitive. Une fois cette période passée, le prestataire doit procéder à la destruction des fichiers supports ;

- mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) ;
- définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé ;
- authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative ;
- assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant ;
- assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport ;
- assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement ;
- assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement ;
- renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé ;
- définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin ;
- assurer l'intégrité du système, de l'urne et de la liste d'émargement ;
- s'assurer que le dépouillement de l'urne puisse être vérifié a posteriori ;
- assurer une haute disponibilité de la solution ;
- assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement ;
- permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin ;
- authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative ;
- assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours ;
- utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI ;
- assurer la transparence de l'urne pour tous les électeurs ;

En tout état de cause, la solution devra être totalement conforme aux objectifs de sécurité de la recommandation CNIL pour un risque de niveau 2.

b. Respect de la réglementation sur la protection des données personnelles

Pour les seules nécessités des opérations électorales (notamment l'établissement des listes électorales), l'entreprise sera amenée à transmettre au prestataire des fichiers établis à partir d'extractions des fichiers de gestion du personnel de l'entreprise.

Les traitements des données personnelles opérés dans le cadre des opérations électorales feront l'objet d'une documentation interne d'Orange, conformément à la réglementation applicable en matière de protection des données personnelles.

Il est également demandé que le système intègre les recommandations de la CNIL de niveau 2 présentées en annexe. Une analyse d'impact (PIA) visée à l'article 35 du Règlement sur la protection des données sera conduite. Dans ce cadre, le prestataire pourra être sollicité par l'équipe projet d'Orange.

c. Fourniture d'un rapport d'expertise

Avec la réponse à la présente consultation, le prestataire fournira à Orange les conclusions du rapport d'expertise de son système de vote électronique, réalisé par un expert indépendant. Cet expert indépendant devra répondre aux critères suivants :

- être un informaticien spécialisé dans la sécurité ;
- ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- avoir suivi une formation certifiée portant sur la protection des données pour le vote électronique.

Le prestataire devra permettre la réalisation d'une expertise indépendante complémentaire réalisée nécessairement après la dernière modification substantielle de la conception du système de vote, tel qu'il sera mis en œuvre pour le scrutin Orange dans le cadre du processus de vote. L'expertise réalisée doit avoir procédé au minimum à la vérification du respect par le système de vote des articles R.2314-5 à R.2314-8 du code du travail. Cela recouvre notamment le fait qu'il existe un cahier des charges qui respecte les articles R.2314-6 et suivants, la confidentialité et la sécurité du dispositif, l'accessibilité aux données et la présence de fichiers dédiés.

En complément, dans le cas où Orange déciderait de faire réaliser sa propre expertise indépendante, le prestataire s'engage à donner accès à l'ensemble des informations nécessaires pour la réalisation d'une expertise par un expert indépendant de la solution de vote conformément à la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement, l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des éléments décrits dans la délibération et notamment sur :

- le code source correspondant à la version du logiciel effectivement mise en œuvre ;
- les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
- le système informatique sur lequel le vote va se dérouler ;
- les échanges réseau ;

- les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
- les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;
- l'évaluation du niveau de risque du scrutin ;
- la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.

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

Le rapport d'expertise, et ses annexes seront remis au responsable de traitement et au prestataire de solution de vote par correspondance électronique via Internet.

L'expert fournira un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il sera tenu de prendre toutes dispositions et précautions utilisées afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

Le prestataire s'engage à tenir à la disposition de la CNIL le cas échéant tout rapport d'expertise relatif au système de vote destinés à vérifier le respect des articles R.2314-5 à R.2314-9 du code du travail.

2/ Système de vote électronique distant

Le système de vote électronique sera hébergé (en France) chez le prestataire externe ou chez un fournisseur d'hébergement et sera rendu accessible aux électeurs de manière sécurisée.

Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés.

Le prestataire devra garantir que toutes les mesures physiques seront prises tant au niveau des serveurs du dispositif que sur les postes accessibles au public afin de garantir la sécurité des données personnelles et du système de vote dans son ensemble. En particulier, le prestataire devra répondre aux exigences liées à la sécurité des données personnelles définies : par les autorités (CNIL, ANSSI ...) par Orange et par l'audit réalisé. Les données échangées entre le prestataire et Orange seront transmises par un système d'échange sécurisé.

Les algorithmes de chiffrement et de signature électronique devront être des algorithmes publics réputés « forts ». Si un système matériel permet d'héberger plusieurs scrutins, il devra être mis en

œuvre une solution technique permettant d'isoler chaque scrutin sur un système informatique distinct de manière à garantir que chaque système soit indépendant et se comporte de manière autonome.

Le prestataire s'engage à répondre aux exigences de la politique de Sécurité d'Orange conformément à la fiche ISA (jointe en annexe).

En plus de l'expertise indépendante pourra être commanditée par Orange, Orange pourra par ailleurs réaliser, si nécessaire :

- une analyse de risques sécurité ;
- des tests d'intrusions web sur le service ;
- un audit système ou de configuration des serveurs qui hébergent le service.

3/ Disponibilité du système de vote électronique

Le prestataire assurera la mise en ligne du système de vote électronique durant la période des élections. Durant cette période, le système sera disponible 24h/24.

Le prestataire mettra en œuvre les moyens d'assurer un service continu, sans rupture, en prévoyant un nombre de connections simultanées suffisamment dimensionné avec un **minimum de 10 000 connections simultanées** et des dispositifs de gestion des débordements pour garantir une expérience utilisateur de qualité sur la totalité de la période de vote.

En cas d'indisponibilité du site de vote ou dysfonctionnement, le système de vote doit permettre de mettre en œuvre une mesure de suspension ou de prorogation du scrutin égale à la durée constatée. Une procédure spécifique doit alors être prévue dans la solution pour permettre la prorogation, en ne levant que les scellés liés à la date de clôture.

La décision de mettre en œuvre cette mesure étant de la prérogative du bureau de vote.

4/ Accessibilité

a. Compatibilité des terminaux

Le prestataire s'assurera que le site de vote soit bien accessible via l'ensemble des outils à disposition des salariés (PC professionnel et personnel, tablette, Smartphone...) mais également avec le respect des normes d'accessibilité, notamment pour les personnes en situation de handicap (ex. malvoyants, non-voyants, handicap moteur).

Le service devra au minimum être compatible avec les spécifications minimales

- Windows 8 et navigateur Firefox ESR 32 ;
- Android 4.3.1 et navigateur Firefox 27.

b. Respect des normes d'accessibilité numérique

Le prestataire s'assurera que le respect des normes d'accessibilité numérique, pour les personnes en situation de handicap, soit pris en compte.

Le prestataire devra se référer à l'annexe accessibilité jointe au présent document.

L'ensemble des contenus numériques fourni par le prestataire devront répondre aux exigences d'accessibilité :

- Site de communication ainsi que les vidéos
- E-mail de sollicitation : l'ensemble des e-mails envoyés aux votants, du 1^{er} jusqu'au mail de confirmation
- Site de vote : le site de démonstration et le site de production devront être identiques et accessibles. Si un mécanisme de CAPTCHA est mis en place, ce dernier devra respecter les normes d'accessibilité citées en annexe.

Conformément à la loi, le site devra afficher une déclaration d'accessibilité qui affiche le taux de conformité à la norme. Orange impose une présentation pour ces déclarations (exemple : <https://www.orange.fr/accessibilite?url=app.visualvoicemail.android.orange.fr>) et propose une méthode appelée la Va11ydette (<https://la-va11ydette.orange.com/?list=wcag-web&lang=fr>). Cette déclaration sera de préférence réalisée par le prestataire puis vérifiée par le centre de compétences accessibilité d'Orange. Elle doit être accessible via un lien « accessibilité » dans le pied de page du site. Tout nouveau site doit être proche d'une conformité à 100%.

5/ Accès aux informations sur les matériels et dans les locaux du prestataire

Le prestataire indiquera comment sont protégés :

- les locaux d'hébergement des matériels sur lesquels sont stockés les fichiers sensibles tels que le fichier des électeurs, les urnes électroniques et les émargements ;
- de manière générale, les informations liées à la gestion des élections d'Orange.

Le système de vote est hébergé en France.

V – Préparation des élections

1/ Contribution du prestataire aux modalités d'organisation des élections

Le prestataire fournira **soutien et conseil** tout au long des différentes phases du processus électoral. Il devra notamment être attentif et intégrer dans la solution de vote fournie sur toutes les dispositions prévues dans le protocole d'accord préélectoral.

Le prestataire s'engage par ailleurs à fournir un accompagnement via des préconisations et argumentations sur les solutions retenues lors de l'élaboration des modalités électorales au travers notamment de :

- propositions de documents types : courriers, notices de vote... ;
- arguments sur éléments techniques liés au site de vote : taille maximum des logos, visibilité de tous les logos sur une seule et même page, navigation au sein du site de vote.... ;
- éléments liés au vote lui-même : modalités d'envoi des codes, modalités de validation des votes..... ;
- proposition d'un espace de communication sur le site de vote : son organisation, élaboration d'une vidéo, affichage des listes et conception push mail (HTML).

Le prestataire s'engage à signaler par écrit à l'équipe projet sous 48 heures à compter de la réception des différents documents communiqués par Orange les questionnements et ou les éventuelles incompatibilités avec le système de vote.

A défaut de réponse dans les 48 heures, les fonctionnalités et modalités inscrites dans les documents fournis seront réputées compatibles avec le système de vote proposé par le prestataire.

Le prestataire fera une présentation du système de vote aux Organisations Syndicales.

Le prestataire s'engage à fournir une notice d'information comportant une description détaillée du système de vote et du déroulement des opérations électorales.

Le prestataire s'engage enfin à ce que le système de vote électronique proposé soit conforme à l'ensemble des exigences légales et réglementaires en vigueur.

2/ Phase de test et de recette du système de vote électronique

Le prestataire devra proposer les moyens de tester l'ensemble des scénarios durant une période prévue dans un calendrier de préparation des élections.

Cette période de test sera déterminée d'un commun accord entre Orange et le prestataire. Elle sera prévue à l'issue de la phase de paramétrage et de préparation du système de vote électronique.

Les fichiers de données de tests fournis par Orange pour la recette seront :

- Organisation
- Electeurs CSEE

En aucun cas, Orange ne peut s'engager à fournir les fichiers de données réels, définitifs et complets pour la phase de recette. Les électeurs et les candidats du jeu de données seront constitués de données fictives. Le jeu de données pour la recette sera néanmoins représentatif en termes de volumétrie.

Les tests programmés dans cette phase permettront notamment de contrôler le déroulement et la conformité du scénario de vote pour chaque élection.

Le prestataire fournira à l'issue de chaque phase de tests un rapport détaillé du déroulement et résultats de tests précisant tous les éléments nécessaires (description des plateformes, jeux de données utilisés, description des scénarios de tests, ...) et permettant de qualifier les résultats obtenus.

3/ Listes électorales

Le système retenu garantit la confidentialité des données transmises par Orange au prestataire, notamment celle des fichiers constitués pour établir les listes électorales ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

Les moyens d'authentifications devront être adressés aux électeurs par deux canaux distincts.

a. Constitution des fichiers

Les listes électorales sont constituées par Orange. Elles comportent les informations nominatives des électeurs ayant la possibilité de participer aux élections. Elles sont établies par collège et par Etablissement Distinct.

La description de l'organisation en Etablissement Distinct sera fournie au prestataire.

Elles seront transmises au prestataire par transfert sécurisé à partir d'un outil interne à Orange.

Une fois fiabilisées, les listes électorales doivent permettre :

- d'éditer les listes électorales à afficher par Etablissement Distinct et par collège;
- d'attribuer à chaque électeur autorisé des codes d'authentification pour accéder au système de vote électronique pour chaque électeur autorisé ;
- de contrôler les accès au système de vote électronique ;
- d'enregistrer les émargements électroniques après chaque vote et assurer l'unicité du vote pour chaque électeur ;
- d'éditer les listes d'émargement ;
- d'envoyer les différents courriers et pushmails.

Pour tout fichier transmis et après injection dans le système de vote, le prestataire devra s'assurer de la fiabilité et de la conformité des données injectées par lui dans le système de vote par rapport aux données transmises par Orange.

Un exemple de ces fichiers sera fourni par Orange au prestataire pour la réalisation de tests.

b. Confidentialité des fichiers

Le prestataire s'engagera à conserver de manière confidentielle toutes les informations et les données qui lui seront transmises pour les besoins de gestion du vote électronique. Il mettra en œuvre tous les moyens nécessaires afin de sécuriser l'accès aux informations de ce fichier sur

ses propres systèmes et à strictement limiter leur consultation aux seuls personnels chargés de la gestion et de la maintenance du vote électronique

c. Mise à jour des listes électorales

Les listes électorales pourront subir des modifications jusqu'au scellement des urnes notamment pour la suppression ou l'ajout d'électeurs.

Pendant toute l'ouverture de la plateforme hébergeant les listes électorales et jusqu'au scellement, le prestataire devra s'assurer qu'Orange puisse :

- consulter les listes électorales et les données électeurs ;
- modifier par IHM et par import de fichier des données électeurs, y compris le collège électoral, et le positionnement de l'électeur dans l'organisation ;
- extraire les listes électorales.

Les modifications des données salariés seront traitées par la Direction des Relations Sociales Groupe.

Lorsque les modifications sont réalisées après l'affichage des listes électorales définitives, le prestataire devra s'assurer que les codes d'accès fournis à des électeurs supprimés des listes soient invalidés, et que les nouveaux électeurs inscrits sur les listes puissent disposer dans un temps utile la notice d'information sur les opérations électorales, des codes d'authentification et des accès nécessaires à leur participation effective au vote électronique.

d. Accès aux listes électorales sur le site de gestion de l'organisateur du scrutin

Le prestataire devra permettre à Orange d'accéder aux listes électorales dès leur injection dans le site de supervision jusqu'à la fin des délais de recours légaux ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive.

Différents profils d'utilisateurs seront définis et communiqués par Orange, auxquels seront associés des droits différents.

Le prestataire devra notamment prévoir d'ouvrir le site de supervision avant la publication des listes électorales provisoires, afin de permettre un accès restreint aux listes électorales :

- la fiche électeur devra être masquée ;
- les utilisateurs pourront faire des recherches et des tris ;
- le téléchargement de ces listes électorales ne sera pas possible.

Le prestataire devra garantir un volume de connexions à plus de **1 000 utilisateurs** (sous réserve de contrainte technique).

4/ Liste de candidats

a. Constitution des fichiers

Les listes de candidats sont constituées par les organisations syndicales au sein de l'UES au 1^{er} tour. La constitution de listes de candidats étant libre au 2nd tour, les listes peuvent être constituées par toute personne remplissant les conditions posées par le législateur.

b. Injection des fichiers dans le système de vote

Les listes de candidats seront transmises au prestataire par transfert sécurisé en vue de leur implémentation automatique dans le système de vote électronique afin d'éviter toute saisie manuelle.

Dès lors que les fichiers fiabilisés lui seront transmis et après injection par lui dans le système de vote, le prestataire devra s'assurer de la fiabilité et de la conformité des données injectées par rapport aux données transmises par Orange.

Orange sera responsable de la qualité des référentiels de données métier fournies en amont pour alimenter la solution de vote en ligne du prestataire.

Le prestataire sera garant et responsable de la qualité des traitements qu'il réalise sur ces données à des fins de paramétrage ou d'initialisation de sa solution de vote :

- le prestataire devra mettre en place des tests de vérification de la complétude et de l'exactitude des données injectées dans la solution sur la base du référentiel de données fournies par Orange ;
- le prestataire devra préciser les moyens et les phases du projet prévus pour réaliser ces tests.

Si une anomalie détectée est liée à la qualité des données contenues dans les fichiers fournis par Orange, alors Orange est responsable de cette anomalie. A l'inverse, si l'anomalie détectée est liée à la qualité des traitements faits sur les données par le prestataire, ce dernier est responsable de cette anomalie.

Le prestataire devra également s'assurer que les logos et professions de foi sont bien affichés dans l'ordre du tirage au sort transmis par Orange et rattachés aux listes correspondantes.

Un fichier sera fourni par Orange au prestataire pour la réalisation de tests.

Le prestataire devra prévoir un temps pour permettre aux organisations syndicales de contrôler la fiabilité, la cohérence et l'affichage des données à publier.

c. Format des fichiers

Le format des listes de candidats pour chacun des scrutins sera transmis au prestataire.

5/ Génération et envoi des informations relatives aux élections

a. Courriers et push mails

A partir des référentiels de données fournies par Orange, le prestataire assurera la réalisation et la transmission à chaque électeur des éléments suivants :

- une lettre d'annonce des élections contenant un extrait des listes électorales de chaque salarié pour contrôle et validation ;
- les modalités de connexion de vote par internet (code d'accès) accompagné de la notice de vote d'information détaillée sur le déroulement des opérations électorales ;
- un lien vers l'espace de communication des élections Orange ;
- les professions de foi ;
- l'annonce de l'ouverture du processus électoral et les relances.

La transmission de ces informations pourra se faire selon les options qui seront retenues dans les modalités électorales :

- sous format électronique ;
- sous format papier.

Pour l'envoi des courriers sous format papier, le prestataire devra respecter un délai maximum de 15 jours à compter de l'envoi des fichiers par Orange (vérification, impression et envoi des courriers).

Pour chacun de ces envois, l'électeur ne devra avoir accès qu'aux données et professions de foi qui le concerne, sauf pour les listes électorales.

b. Codes d'accès au système de vote électronique

Chaque électeur recevra de manière sécurisée :

- un identifiant unique d'accès qui permettra, outre le contrôle d'accès, la tenue des listes d'émargement électroniques garantant de l'unicité des votes ;
- un mot de passe qu'il sera seul à connaître, ce code sera unique pour valider chacun des votes sur chacun des scrutins auquel l'électeur sera amené à participer.

L'envoi de l'identifiant et du code d'accès doivent se faire impérativement par deux canaux différents.

Dans le respect de l'anonymat, le prestataire proposera des procédures de génération et de transmission des codes d'accès aux électeurs permettant de conserver le caractère confidentiel du mot de passe durant toutes les étapes.

Ainsi en cas de perte de ses codes de votes, un électeur aura la possibilité d'en demander des nouveaux en ligne via un espace sécurisé.

Les nouveaux codes seront transmis à l'électeur par mail ou SMS. En cas de problème de réception, le prestataire devra proposer une solution alternative permettant à l'électeur de pouvoir voter tout en garantissant la sincérité du vote.

Le prestataire devra proposer des solutions de contrôle.

En tout état de cause, le système retenu assurera la confidentialité des données transmises à chaque étape du processus ainsi que la sécurité de l'adressage des moyens d'authentification.

6/ Espace de communication

a. Contenu de l'espace de communication

Au sein du site de vote, se trouvera également un espace de communication paramétré par le prestataire intégrant les communications de la Direction ainsi que celles des différentes organisations syndicales, avec une visibilité de tous les logos sur une seule et même page.

Chaque électeur pourra y trouver l'ensemble des informations relatives aux différents scrutins (dates des élections et nature des scrutins) mais également l'ensemble des professions de foi relatives aux scrutins qui le concernent.

Il aura également à sa disposition :

- une vidéo réalisée par le prestataire pour permettre à l'électeur d'appréhender le fonctionnement de la solution de vote ;
- un site de démonstration pour permettre à chaque électeur de tester le dispositif de vote dans des conditions réelles.
- les listes électorales ;
- les listes de candidats.

b. Accès aux listes électorales

Le prestataire assure un accès sécurisé aux listes électorales provisoires à tous les salariés, même s'ils ne figurent pas sur les listes électorales en créant un code d'accès générique par Etablissement Distinct par exemple.

Le prestataire assure un accès sécurisé aux listes électorales définitives et restreint aux électeurs.

En tout état de cause, les listes électorales doivent pouvoir être visionnées sans **être téléchargées**. Les listes visionnées doivent être publiées dans **un format empêchant la reproduction** (ex. protection contre le copier-coller).

7/ Formation

Le prestataire proposera et dispensera une formation sur système de vote à l'ensemble des membres des bureaux de vote tels que défini dans les modalités de vote ainsi qu'aux membres des équipes projet élections de la Direction Orange sur plusieurs sessions.

VI- Le vote

1/ Organisation des bureaux de vote

Dans le cadre des opérations électorales électronique, il devra y avoir un bureau de vote électronique (BVE) centralisateur CSE et un BVE au niveau de chaque Établissement Distinct.

Le BVE centralisateur déverrouille, donne l'autorisation de dépouiller aux BVE Établissements Distincts et supervise le dépouillement des urnes CSEE de l'ensemble de l'UES. Il centralise les résultats des urnes salariés de droit privé et signe les PV.

Les BVE au sein des Établissements Distincts les urnes CSE de l'Établissement Distinct concerné.

2/ Scellement des urnes

Le prestataire s'engage à participer à la réunion de scellement des urnes en présence des représentants des listes de candidats (délégués de listes) et de la direction afin de réaliser les actions suivantes :

- procède avant que le vote ne soit ouvert à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;
- procède avant que le vote doit ouvert à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;
- contrôle à l'issue des opérations de vote et avant les opérations de dépouillement le scellement de ce système.

Le système de vote électronique doit être scellé à l'ouverture et à la clôture du scrutin. Le contrôle du scellement doit pouvoir être effectué à tout moment durant la période de vote par les membres du bureau de vote centralisateur, tel que défini dans le protocole d'accord préélectoral.

Ce système pourra être scellé en présence d'huissiers. La procédure de scellement devra être clairement exposée en amont et être scrupuleusement respectée.

Lors de la procédure de scellement, il sera réalisé un scrutin à blanc, sur au minimum 3 Etablissements Distincts comportant au moins 3 salariés de chaque collège par scrutin.

Le scrutin à blanc vise à contrôler et valider les scénariis d'élections et la bonne intégration des listes de candidats et des professions de foi.

Il doit être effectué sur le système de vote électronique définitif et validé préalablement, afin de permettre aux membres du bureau de vote centralisateur de contrôler la conformité du système de vote électronique avant l'ouverture effective des élections.

Le « scrutin à blanc » vise à tester l'application en fonctionnement réel. Durant cette phase, les membres du bureau de vote centralisateur pourront tester toutes les phases de vote des élections.

Pour ce faire, les membres des bureaux de vote ouvriront les scrutins, effectueront des votes, fermeront les scrutins et dépouilleront les votes effectués.

Au terme de ce test, les membres des bureaux de vote valideront l'intégrité du dispositif.

Tout au long du scrutin, le contrôle du scellement permettra aux membres du bureau de vote centralisateur de s'assurer que l'application n'a été sujette à aucune intrusion.

Les étapes de contrôle seront les suivantes :

- création de 3 clés qui permettront le chiffrement des bulletins de vote dans le système de vote électronique du prestataire. Seules 2 de ces clés seront nécessaires au dépouillement ;
- ouverture des élections ;
- réalisation de plusieurs votes ;
- clôture des élections ;
- remise des clés aux membres du bureau de vote centralisateur permettant le déchiffrement des bulletins de vote. Ces clés pourront ensuite être remises pour conservation jusqu'au jour du dépouillement à un ou plusieurs huissiers ;
- déroulement du dépouillement des urnes électroniques et édition des résultats ;
- contrôles de la conformité des résultats obtenus ;
- scellement de l'application de vote électronique.

Un mode en distanciel sera prévu si besoin (dont les modalités de mise en œuvre devront être précisées par le prestataire).

Une fois le scellement définitif réalisé, un PV de scellement sera généré. Ce PV sera signé par les membres du bureau de vote centralisateur.

3/ Durée du vote

La durée de vote des deux tours de scrutin sera déterminée dans l'accord portant sur la date des élections CSE 2023 au sein de l'UES Orange.

Ces élections auront lieu dans les 15 jours précédant la date de fin de la mandature 2019-2022, fixée au 3 décembre 2023 inclus.

4/ Vote électronique

a. Chiffrement des bulletins de vote dans l'urne électronique

Lors de l'élection par vote électronique, les fichiers comportant les éléments d'authentification des électeurs et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système. A l'inverse, les clés de déchiffrement ne sont pas accessibles par les personnes chargées de la gestion et de la maintenance mais uniquement par les porteurs membres du bureau de vote électronique centralisateur.

Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

Les bulletins de vote enregistrés dans le système de vote électronique doivent être chiffrés avec un algorithme « fort ». Le déchiffrement des bulletins sera assuré par une clé générée par le système de vote et dont les fragments seront confiés lors du scellement aux porteurs (membres du bureau de vote centralisateur) et supprimés des serveurs après leur génération. Ces fragments de clés ou les mots de passe qui les protègent pourront être remis à un ou deux huissier(s) de justice. Dans le cadre d'un recours éventuel au distanciel, le prestataire proposera une modalité de transmission sécurisée aux huissiers.

b. Dispositifs de secours

Le système de vote électronique sera dupliqué sur 2 plateformes distinctes hébergées en France.

En cas de panne d'un des systèmes, un dispositif de secours prendra le relais en offrant les mêmes garanties et les mêmes caractéristiques.

En cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données, le bureau de vote centralisateur aura compétence, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote.

c. Scénario de vote

Le scénario de vote électronique comportera les étapes suivantes pour chaque scrutin :

- une étape d'identification de l'électeur ;
- une étape de présentation des scrutins ;
- une étape de présentation des listes de candidatures en présence ;
- la possibilité pour l'électeur de consulter les professions de foi de toutes les listes liées au scrutin sur lequel il a entamé le processus de vote ;
- le choix par l'électeur d'une seule liste parmi celles proposées, ou bien le choix de voter « blanc » ;
- la présentation du bulletin de vote définitif comprenant les candidats ;
- en cas de rature ou de décochage d'un ou plusieurs candidats sur le bulletin de vote, l'électeur sera alerté par une fenêtre « pop up » lui permettant de confirmer son ou ses choix pour les candidats concernés ;
- la confirmation par l'électeur du choix effectué via la saisie de son mot de passe pour chaque vote ;
- la confirmation à l'électeur par le système de la prise en compte de son bulletin de vote ;
- la possibilité pour l'électeur d'imprimer un accusé de réception confirmant l'enregistrement de son vote et attestant de la prise en compte de ses suffrages par le système de vote. Cette possibilité lui sera offerte à l'issue de la séquence de vote mais aussi ultérieurement, en se reconnectant à l'application. Il mentionnera les élections concernées ainsi que la date et l'heure d'émission de chaque suffrage. Cet accusé de réception comportera une marque d'authentification interdisant une édition frauduleuse.

d. Enchaînement des élections

Le système de vote proposera automatiquement à l'électeur de poursuivre le déroulement du scénario afin de réaliser le vote suivant sur le même site. L'électeur pourra se connecter tant qu'il n'aura pas épuisé les votes qui lui sont proposés.

L'électeur ne doit voir que les scrutins (Titulaires/Suppléants de son Etablissement Distinct et de son collège) pour lesquels il est concerné.

e. Émargement électronique, unicité du vote

Par ailleurs, le système de vote électronique enregistrera un émargement après confirmation du vote par l'électeur, via la saisie de son mot de passe, et ne permettra plus à ce dernier d'effectuer un nouveau vote pour cette même élection (unicité du vote).

L'émargement indique la date et l'heure du vote. Les listes sont enregistrées sur un support distinct de celui de l'urne électronique, scellé, non réinscriptible, rendant son contenu inaltérable et probant.

La liste d'émargement comprendra :

- les noms et prénoms des électeurs ;
- le libellé du scrutin (1^{er} ou 2nd tour) ;
- le collège de l'électeur ;
- l'heure.

Les listes d'émargement seront disponibles en lecture **sans possibilité de téléchargement** pendant le scrutin et seront mise à jour toutes les heures. Les qualités des personnes qui auront accès à celles-ci seront définies dans le protocole d'accord préélectoral.

Le prestataire s'engage à mettre en place un CAPTCHA pour déceler tout chargement de données en fort volume.

f. Taux de participation

Le prestataire fournira un taux de participation de façon dynamique à la maille de chaque Etablissement Distinct pour chaque scrutin.

5/ Assistance technique

Durant le scrutin, un interlocuteur dédié du prestataire se tiendra en permanence à la disposition des représentants de la direction et des membres du bureau de vote national et assurera également la surveillance du système de vote électronique.

6/ Assistance téléphonique salariés

Un service d'assistance téléphonique (hotline salarié) sera mis en œuvre, avant et pendant les opérations électorales, dans le but de renseigner les électeurs mais également pour traiter les réclamations.

Cette hotline devra être suffisamment dimensionnée pour gérer l'ensemble des flux d'appels sur toute la durée du vote. Elle devra pouvoir être instantanément redimensionnée en cas d'incident amenant un flux d'appels important ponctuel.

Orange fournira au prestataire un modèle de fichier pour les réclamations.

VII – Dépouillement et résultats

1/ Dépouillement des urnes électroniques et déchiffrement des bulletins de vote

Le dépouillement s'effectuera après la clôture des scrutins et ne pourra commencer qu'une fois les fragments de clés de déchiffrement entrées par 2 membres du bureau de vote centralisateur. Lors de la cérémonie de dépouillement, le président puis les assesseurs, via un poste connecté à internet, introduisent leurs clés de déchiffrement et saisissent le mot de passe associé.

Ceci aura pour but de déverrouiller les urnes et ainsi avoir accès à :

- l'édition des résultats des élections ;
- la remise par le prestataire des procès-verbaux complétés et conformes aux modèles CERFA. Chaque CERFA devra mentionner tous les numéros de SIRET des établissements rattachés à l'Etablissement Distinct.

L'ensemble des étapes décrites ci-dessus seront être réalisées en présence d'Huissiers.

2/ Remise des résultats

Les résultats seront consultables dès le dépouillement des urnes électroniques.

Seuls les membres désignés du bureau de vote ainsi que les représentants de l'employeur habilités auront accès à ces résultats.

3/ Données à fournir à l'issue de la consolidation des résultats

a. Les résultats

Les fichiers de résultats comporteront à minima :

- le décompte des voix par élection ;
- le nombre d'électeurs inscrits ;
- le nombre de votants ;

- le nombre de bulletin blancs ou nuls ;
- le nombre de suffrages valablement exprimés,
- le nombre de voix obtenu par chaque liste ;
- la représentativité de chaque organisation syndicale.

A l'issue des négociations préélectorales les données produites pourront être enrichies.

b. Procès-verbaux des élections

Les Procès-verbaux qui doivent être conformes aux prescriptions légales pourront être édités par Orange depuis la solution de vote. Les résultats y seront affichés et classés selon un ordre défini en amont par tirage au sort.

Ils seront mis à disposition d'Orange par le prestataire.

En complément, pour le premier tour des élections CSE **titulaires uniquement**, il sera distingué au sein d'urnes séparées les votes des salariés de droits privés et ceux des fonctionnaires pour la représentativité calculée au niveau de la branche des télécoms. Les PV des résultats du scrutin des seuls salariés de droit privés aux élections professionnelles CSE de l'UES Orange par établissement et par collège sera mis à disposition des membres du bureau de vote centralisateur pour signature.

c. Listes d'émargement

Les listes d'émargement définitives pourront être éditées par Orange à l'issue des élections et seront accessibles en cours de scrutin par les membres du bureau de vote et les délégués de liste à des fins exclusives de contrôle du déroulement du scrutin. **Aucun téléchargement de ces listes d'émargement ne sera rendu possible.**

VIII – Archivage, conservation et destruction des données

Le prestataire conservera les fichiers supports (comprenant la copie des programmes sources et des programmes exécutables, les listes électorales, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde), jusqu'à l'expiration du délai de recours ou lorsqu'une action contentieuse est engagée après qu'une décision juridictionnelle soit devenue définitive. A l'expiration de ces délais, le prestataire s'engagera à détruire tous les fichiers et à ne conserver aucune de ses données suite à une demande explicite du représentant d'Orange. Le prestataire fournira à Orange sans délai à l'issue de cette procédure, un certificat de suppression des données.

Le prestataire fournira également sur support numérique une copie intégrale des résultats.

IX – Trame de réponse de mise en œuvre du vote électronique

Sommaire

1. POINTS FORTS DE L'OFFRE	80
2. DESCRIPTION DE LA SOLUTION PROPOSEE	80
I. ARCHITECTURE FONCTIONNELLE ET TECHNIQUE GENERALE DE LA SOLUTION PROPOSEE	80
II. GESTION DES CLES ET DES SECRETS	80

III.	DISPOSITIONS PRISES DANS L'OFFRE EN MATIERE DE DEVELOPPEMENT DURABLE	80
IV.	DESCRIPTION DE LA SOLUTION DE VOTE ELECTRONIQUE DISTANTE	80
V.	DESCRIPTION DE LA SOLUTION POUR L'ESPACE DE COMMUNICATION	81
VI.	DESCRIPTION DE LA SOLUTION POUR LA GESTION ET L'ENVOI DES SECRETS DE VOTE POUR LES ELECTEURS.....	81
VII.	DESCRIPTION DE LA SOLUTION POUR LA PRISE EN COMPTE DES CANDIDATURES (listes des candidats, logos et professions de foi)	81
VIII.	DESCRIPTION DE LA SOLUTION POUR L'ASSISTANCE TELEPHONIQUE	82
DOCUMENTS ANNEXES.....		82

1/ POINTS FORTS DE L'OFFRE

Pouvez-vous préciser, les points forts de l'offre, au plan :

- De la conformité à la délibération CNIL de 2019 ?
- De l'ergonomie de l'application de vote pour les électeurs ?
- De la génération et de l'utilisation de la preuve de vote ?

2/ DESCRIPTION DE LA SOLUTION PROPOSEE

I.ARCHITECTURE FONCTIONNELLE ET TECHNIQUE GENERALE DE LA SOLUTION PROPOSEE

Quels sont les principaux composants fonctionnels (liste électorale, candidatures, supervision du vote, déroulement du vote,..) et techniques (espace de vote et espace de communication) ?

II.GESTION DES CLES ET DES SECRETS

Quels sont les principes, l'arborescence et les modalités de production et de mémorisation des clés pour les différents composants applicatifs :

- Pour le scellement du code ?
- Pour les chiffrements des scrutins ?
- Pour la génération des identifiants et mots de passe pour les électeurs ?
- Pour les accès des bureaux de vote à la supervision des scrutins ?
- Niveau de conformité des dispositifs proposés pour les traitements avec le Référentiel Général de Sécurité ?

III.DISPOSITIONS PRISES DANS L'OFFRE EN MATIERE DE DEVELOPPEMENT DURABLE

Quelles sont les dispositions particulières de l'offre et de la mise en œuvre de la solution en matière de développement durable ?

IV.DESCRPTION DE LA SOLUTION DE VOTE ELECTRONIQUE DISTANTE

Quels sont les dispositifs de chiffrement utilisés pour les bulletins de vote : algorithme de chiffrement, génération des clés, conservation des clés ?

Pouvez-vous préciser les fonctions disponibles pour l'organisateur du scrutin (fonctions accessibles en préparation des données, lors du scellement, pendant le vote et lors du dépouillement) et pour les membres des bureaux de vote ?

Comment sont produits et utilisables, par les électeurs, la preuve de vote ?

Pouvez-vous décrire et préciser les infrastructures d'hébergement, leur localisation, leurs composants et les dispositifs de sécurité mis en œuvre pour les accès physiques et logiques aux infrastructures utilisées par la solution de vote ?

Comment pouvez-vous démontrer au niveau de l'offre les engagements de performance pendant le vote (en particulier pour l'engagement minimum de 10 000 connections simultanées) et pour le dépouillement ?

Pouvez-vous préciser le détail de la conformité pour chaque objectif de sécurité à la recommandation CNIL 2019 pour un niveau 2 et pour un niveau 3 ?

Pouvez-vous préciser les dispositifs de type SIEM et bastion mis en œuvre pour garantir la traçabilité totale des interventions techniques sur la solution de vote entre le scellement et le dépouillement ?

Quelle est la réponse de l'offre aux exigences de sécurité ISA de Orange ?

V. DESCRIPTION DE LA SOLUTION POUR L'ESPACE DE COMMUNICATION

Quelles sont les fonctionnalités standards de l'espace de communication proposé ? Quels sont les développements complémentaires envisagés ?

VI. DESCRIPTION DE LA SOLUTION POUR LA GESTION ET L'ENVOI DES SECRETS DE VOTE POUR LES ELECTEURS

Comment est géré et réalisé l'envoi des courriers (si cette solution est retenue) ?

Comment est géré et réalisé l'envoi des courriels (si cette solution est retenue) ?

Comment est assuré le ré-assort (renvoi des éléments d'authentification aux électeurs qui en font la demande) ?

VII. DESCRIPTION DE LA SOLUTION POUR LA PRISE EN COMPTE DES CANDIDATURES (listes des candidats, logos et professions de foi)

Comment sont assurés, la prise en compte et la vérification des candidatures par l'organisateur des scrutins et par les OS candidates ?

En cas de saisie des candidatures par les OS déposants, quels sont les workflow de contrôle et de validation ? Comment sont-ils paramétrables et adaptables aux spécificités de Orange ?

VIII.DESCRPTION DE LA SOLUTION POUR L'ASSISTANCE TELEPHONIQUE

Quels sont les dispositifs et la solution retenue pour l'assistance téléphonique pour les électeurs et pour les membres des bureaux de vote ?

- A quelles informations ont accès les télé-opérateurs ?

DOCUMENTS ANNEXES

18.7

En complément, les soumissionnaires préciseront point par point dans des documents annexes à l'offre technique la conformité des solutions proposées dans l'offre avec les dispositions applicables :

- Le référentiel Général de Sécurité (RGS) – annexe 1 à l'offre technique ;
- Le Référentiel Général sur la Protection des Données (RGPD) – annexe 2 à l'offre technique.

Et de vote électronique par Internet avec :

- Le Référentiel Général d'Accessibilité pour les Administrations (RGAA) – annexe 3 à l'offre technique ;
- Une expertise indépendante récente réalisée en réponse aux exigences de sécurité et aux dispositions de la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet pour un risque de niveau 2 (annexe 4 à l'offre technique).

- Cahier des charges de l'accessibilité numérique S3F0

18.8 Introduction

La loi pour une république numérique de 2016 et le décret 2019-768 publié en juillet 2019 imposent aux entreprises dont le chiffre d'affaires annuel est d'au moins 250 millions d'euros de proposer des services numériques accessibles, engagement décrit dans [le schéma pluri-annuel d'amélioration de l'accessibilité d'Orange](#).

L'accessibilité numérique consiste à fournir des produits ou services pouvant être utilisés par tous, sans distinction de situation ou de handicap.

Elle concerne l'ensemble des technologies de l'information et de la communication. Elle couvre différentes technologies comme le Web, les applications mobiles, les vidéos, les documents Office et PDF, la télévision numérique et les objets connectés, et ceci quel que soit le support (ordinateur, tablette, mobile...) ou le domaine (site commercial, e-learning, Intranet d'entreprise, progiciel RH ou financier, outil collaboratif...). Ce périmètre suit les évolutions des services et des technologies numériques.

L'accessibilité numérique s'intéresse à tous les handicaps qui affectent l'accès au numérique, ce qui inclut les utilisateurs ayant une déficience visuelle, auditive, motrice, de parole, cognitive...

18.9 Objectif d'accessibilité du groupe Orange

Concernant les contenus Web, quels que soient le support (ordinateur, mobile, tablette, TV...) et la technologie, l'objectif d'accessibilité du groupe est le respect du **niveau AA des Web Content Accessibility Guidelines* (WCAG) version 2.1**. Ces contenus doivent en outre ne montrer aucun point bloquant du point de vue d'un utilisateur en situation de handicap.

(* Le World Wide Web Consortium (W3C) a lancé en 1996 l'initiative pour l'accessibilité du Web (Web Accessibility Initiative - WAI) pour améliorer l'accessibilité des contenus Web. La WAI a émis des recommandations nommées « règles d'accessibilité pour les contenus Web » ou WCAG (pour l'anglais Web Content Accessibility Guidelines), actuellement en version 2.1, qui constituent le standard international.

18.10 Référentiel

Le standard WCAG 2.1 est disponible en ligne sur [le site du W3C](#).

Orange a créé un site de recommandations dans l'objectif de faciliter l'accès aux standards ou aux bonnes pratiques. Le [site des recommandations accessibilité Orange](#) propose des ressources pédagogiques, des exemples, une méthode de tests et une liste d'outils qui facilitent la prise en compte de l'accessibilité numérique. Ce site évolue régulièrement pour suivre l'évolution des technologies.

18.11 Exemple d'exigences fonctionnelles :

18.11.1 Voici un sous ensemble des exigences du référentiel WGAC 2.1 :

- Pertinence de l'information
 - Images : toujours fournir une description textuelle pertinente
 - Icônes de candidats : s'assurer qu'elles sont complètes
 - Syndicats : pas d'intitulé pour le logo
 - Titres des pages : désambiguïser les titres pour qu'on sache exactement à quel endroit du parcours on est
 - Toujours expliciter le contenu d'une iframe à l'aide de l'attribut title sur la balise iframe.
- Formulaire
 - Indiquer explicitement quels champs sont obligatoires
 - Regrouper les boutons radio
- Navigation au clavier
 - Sauf difficulté exceptionnelle, ne pas ajouter d'attribut tabindex, et si on doit en ajouter un, ne jamais utiliser une valeur supérieure à 0
 - Rendre systématiquement très visible le focus en cas de navigation clavier
- Usage conforme des technologies web
 - En cas d'ajout d'attribut ARIA, s'assurer que l'usage est conforme.
 - Ne pas utiliser de rafraîchissement automatique de la page ou fournir un moyen de prolonger ou de désactiver le compte à rebours.
- Présentation de l'information
 - Toujours permettre à l'utilisateur de zoomer l'interface (ne pas utiliser user-scalable=0 dans le meta viewport). De même s'assurer qu'en cas de zoom tous les contenus sont visibles (pas de chevauchements, pas de contenus qui disparaissent ou sont tronqués).
 - En cas de désactivation (ou de non-chargement) des feuilles de style, le contenu doit rester compréhensible. De même pour cacher un champ on préférera utiliser type=hidden plutôt que class=hidden.
 - Contrastes : s'assurer que tous les contenus ont un contraste suffisant.
 - Expliciter les contenus (Suite = suite de la liste ou étape suivante ?).
 - Doubler systématiquement, pour chaque pictogramme, l'information visuelle d'une information textuelle (ne pas s'appuyer uniquement sur le alt de l'image ou l'aria-label, ajouter systématiquement un title).

18.12 Mesure

À tout moment, l'équipe projet devra présenter des livrables (spécifications / maquettes fonctionnelles, intégrations HTML, environnement de recette et/ou de pré-production, livraison finale...) conformes aux règles d'accessibilité à appliquer au stade de développement considéré, que ce soit pour les éléments graphiques, ergonomiques, fonctionnels, techniques ou éditoriaux.

Avant la mise en production, l'équipe projet devra effectuer des tests accessibilité de validation et les remettre à Orange. Elle corrigera les éventuelles erreurs constatées pour atteindre le niveau exigé.

NB : si des erreurs résiduelles sont constatées par Orange, elles devront être corrigées.

Une vigilance particulière devra être portée sur :

- La conformité à la charte graphique d'Orange, tout particulièrement en matière de contrastes des combinaisons de couleurs entre le contenu et l'arrière-plan.
- La compatibilité avec les aides techniques (lecteurs d'écran tels que Jaws et NVDA, les systèmes de configuration d'agrandissements comme les loupes logicielles).
- L'accessibilité au clavier (touches [Tab] tabulation, [Entrée]...).

Il est demandé au candidat d'indiquer dans sa réponse :

- La méthodologie qu'il propose pour prendre en compte les règles d'accessibilité à toutes les étapes du projet.
- Les livrables qu'il s'engage à fournir pour permettre à Orange d'avoir des garanties sur le niveau d'accessibilité obtenu (tests de recette etc.).
- Les références de projets déjà réalisés et conformes aux exigences d'accessibilité.
- Les mesures prises pour s'assurer d'une compétence suffisante en accessibilité dans ses équipes et les résultats obtenus.
- Tout autre élément permettant d'évaluer l'expertise et l'engagement du candidat en matière d'accessibilité numérique.

18.13 Vérification par Orange

Le niveau de conformité au référentiel d'accessibilité est vérifié par le centre de compétence de l'accessibilité numérique du groupe Orange : conformément à la loi, cette évaluation se traduit par la relecture de la déclaration d'accessibilité informant du taux de conformité au référentiel.

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

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

NOR : CNIL1917529X
JORF n°0142 du 21 juin 2019
Texte n° 95

Version initiale

La Commission nationale de l'informatique et des libertés,
Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;
Vu le code électoral ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-I-2°-a bis) ;
Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Article

Après avoir entendu Mme Dominique CASTERA, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;
Formule les observations suivantes :

A titre liminaire, la commission observe que le constat, réalisé lors de l'adoption de sa recommandation de 2010, du développement et de l'extension des systèmes de vote par correspondance électronique, notamment via Internet, à un nombre croissant d'opérations de vote et de types de vote, reste d'actualité.

La commission souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel et libre du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote par correspondance électronique, notamment via Internet, doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Devant l'extension continue du vote par Internet à tous types d'élections, la commission souhaite rappeler que le vote par correspondance électronique, notamment via Internet, présente des difficultés accrues au regard des principes susmentionnés pour les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement, principalement à cause de l'opacité et de la technicité importante des solutions mises en oeuvre, ainsi que de la très grande difficulté de s'assurer de l'identité et de la liberté de choix de la personne effectuant les opérations de vote à distance.

Au cours des travaux que la commission a menés depuis 2003 et compte tenu des menaces qui pèsent sur ces dispositifs, elle a, en effet, pu constater que les systèmes de vote existants ne fournissaient pas encore toutes les garanties exigées par les textes légaux. Dès lors et en particulier, compte-tenu des éléments précités, la commission reste réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment via Internet, pour des élections politiques.

La présente délibération a pour objet de revoir la recommandation de 2010 à l'aune des opérations électorales intervenues depuis, de l'évolution des solutions de vote proposées par les prestataires du secteur, des retours effectués par les différentes parties prenantes, des contrôles réalisés par la CNIL ainsi que de l'évolution du cadre juridique relatif à la protection des données.

La nouvelle recommandation a pour champ d'application les dispositifs de vote par correspondance électronique, en particulier via Internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les systèmes informatiques mis à disposition des votants sous forme de boîtiers de vote ou en isolements (dites « machines à voter »). Elle est destinée à fixer, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment via Internet, en fonction des risques que présente le déroulement du vote. Les réponses apportées par les systèmes à ces objectifs de sécurité doivent ainsi prendre en compte le contexte et les menaces qui pèsent sur le scrutin.

Elle vise également à s'appliquer aux futures évolutions des systèmes de vote par correspondance électronique, notamment via Internet, en vue d'un meilleur respect des principes de protection des données personnelles, et à éclairer les responsables de traitement sur le choix des dispositifs de vote par correspondance électronique à retenir.

Elle abroge la délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

Compte tenu de ces observations préalables, la commission émet la recommandation suivante.
Le niveau de risque du scrutin

Le niveau de risque que présente le déroulement d'un vote varie en fonction du type de scrutin, des événements redoutés et des menaces qui pèsent sur le traitement. Ainsi, la commission recommande que la solution utilisée pour le scrutin tienne compte de l'importance du niveau de risque de l'élection ainsi que des éventuels bénéfices pour les parties prenantes de recourir à un système de vote par correspondance électronique et que la solution choisie réponde à tous les objectifs de sécurité fixés au regard de ce niveau de risque.

La commission identifie trois niveaux de risque :

- Niveau 1 : Les sources de menace, parmi les votants, les organisateurs du scrutin ou les personnes extérieures, ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni électeur, ni candidat. Il est considéré comme neutre par toutes les parties. Ce niveau s'applique pour les scrutins impliquant peu d'électeurs, se déroulant dans un cadre non conflictuel, à l'issue duquel les personnes élues auront peu de pouvoirs, comme par exemple l'élection d'un représentant de classe. Le scrutin ne présente pas de risques importants.

- Niveau 2 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique à des scrutins impliquant un nombre important d'électeurs et présentant un enjeu élevé pour les personnes mais dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel. Le scrutin présente un risque modéré.

- Niveau 3 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel. Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important.

La commission déconseille d'utiliser un dispositif de vote par correspondance électronique, notamment via Internet, dans l'hypothèse où les sources de menace peuvent disposer à la fois de ressources importantes et d'une motivation forte.

Le responsable du traitement identifie le niveau correspondant à sa situation en fonction des risques soulevés par son scrutin. A cette fin la commission propose, de manière facultative et à titre d'exemple, une grille d'analyse simplifiée, basée sur des questions fermées, ayant pour objet de guider et d'aider les responsables de traitement le désirant à se positionner sur cette échelle. Cette grille d'analyse est placée au sein de la fiche pratique.

En cas de doute entre deux niveaux, le niveau le plus élevé devrait être privilégié. Le responsable de traitement, maîtrisant le périmètre, les enjeux et le contexte de son scrutin, est libre de choisir le niveau de risque qu'il juge approprié, dès lors qu'il peut justifier son analyse auprès de la commission et de l'expert indépendant.

Une fois son niveau de risque identifié, le responsable de traitement peut déterminer les objectifs de sécurité que la solution de vote doit atteindre.

Le choix du niveau de risque par le responsable de traitement étant évalué par l'expert indépendant mandaté (voir ci-après) pour garantir la conformité des opérations de vote à la présente recommandation, il convient que le responsable de traitement lui fournisse les éléments ayant été pris en compte dans la détermination de ce niveau.

D'une manière générale, la commission rappelle que les traitements de données personnelles, dont les dispositifs de vote, qui remplissent au moins deux des critères suivants doivent en principe faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) :

- évaluation/« scoring » (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles (opinions politiques et appartenances syndicales notamment) ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une technologie nouvelle) ;
- exclusion du bénéficiaire d'un droit/contrat.

Dès lors, au regard des critères relatifs aux données sensibles et à la collecte de données à large échelle et compte tenu du contexte du scrutin le cas échéant, il peut être nécessaire que le responsable de traitement réalise une AIPD.

Les objectifs de sécurité à atteindre en fonction du niveau de risque

Chaque niveau de risque se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité attendu.

Ces objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

La commission proposera sur son site web ou tout autre support utile, une fiche pratique présentant des exemples permettant d'atteindre les objectifs de sécurité précités. Les industriels peuvent, s'ils le souhaitent, proposer à la commission des exemples de moyens permettant d'atteindre les objectifs afin que cette fiche puisse être agrémentée de ces informations. La commission sera seule juge de la pertinence des moyens proposés.

Cette fiche détaillera ce qui est attendu derrière chaque objectif de sécurité.

Les solutions de vote dont le scrutin présente un risque de niveau 1 doivent atteindre a minima l'ensemble des objectifs de

- Objectif de sécurité n° 1-01 : Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).
- Objectif de sécurité n° 1-02 : Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.
- Objectif de sécurité n° 1-03 : Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduits de manière significative.
- Objectif de sécurité n° 1-04 : Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.
- Objectif de sécurité n° 1-05 : Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.
- Objectif de sécurité n° 1-06 : Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.
- Objectif de sécurité n° 1-07 : Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement.
- Objectif de sécurité n° 1-08 : Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.
- Objectif de sécurité n° 1-09 : Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.
- Objectif de sécurité n° 1-10 : Assurer l'intégrité du système, de l'urne et de la liste d'émargement.
- Objectif de sécurité n° 1-11 : S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.

Les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre a minima l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants :

- Objectif de sécurité n° 2-01 : Assurer une haute disponibilité de la solution.
- Objectif de sécurité n° 2-02 : Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.
- Objectif de sécurité n° 2-03 : Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.
- Objectif de sécurité n° 2-04 : Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.
- Objectif de sécurité n° 2-05 : Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
- Objectif de sécurité n° 2-06 : Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.
- Objectif de sécurité n° 2-07 : Assurer la transparence de l'urne pour tous les électeurs.

Les solutions de vote dont le scrutin présente un risque de niveau 3 doivent atteindre a minima l'ensemble des objectifs de sécurité des niveaux 1 et 2, ainsi que les suivants :

- Objectif de sécurité n° 3-01 : Etudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.
- Objectif de sécurité n° 3-02 : Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.
- Objectif de sécurité n° 3-03 : Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.
- Objectif de sécurité n° 3-04 : Permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.
- Objectif de sécurité n° 3-05 : Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.

Le responsable de traitement ou son prestataire sont libres d'utiliser toute solution leur permettant d'atteindre les objectifs de sécurité énoncés.

Quel que soit le niveau déterminé, il convient de fournir aux électeurs, en temps utile, une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote par correspondance électronique, notamment via Internet. Cette notice explicative ne se substitue pas à l'obligation d'information imposée par les articles 13

et 14 du règlement européen sur la protection des données (RGPD) s'agissant du traitement des données. Parallèlement, la commission tient à souligner que, de par leur nature et sensibilité, les plateformes de vote par correspondance électronique, notamment via Internet, se doivent d'être accessibles à toutes personnes, notamment aux personnes en situation de handicap et en particulier visuel. Ainsi, pour les organismes du secteur public ou délégataires d'une mission de service public désirant proposer ce service à ses électeurs, il est nécessaire que le système de vote respecte le référentiel général d'accessibilité pour les administrations (RGAA). Pour les organismes non soumis à ce référentiel, il est fortement recommandé d'en suivre les prescriptions afin de mettre l'ensemble des votants en capacité d'exprimer leur suffrage par ce moyen.

L'expertise du système de vote par correspondance électronique, notamment via Internet

Tout responsable de traitement mettant en oeuvre un système de vote par correspondance électronique, notamment via

Internet, doit faire expertiser sa solution par un expert indépendant, que la solution de vote soit gérée en interne ou fournie par un prestataire.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes

d'électeurs et leur enrôlement et l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des éléments décrits dans la présente délibération et notamment sur :

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

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.

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

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- être un informaticien spécialisé dans la sécurité ;
- ne pas avoir d'intérêt dans la société qui a créé la solution de vote à expertiser, ni dans l'organisme responsable de traitement qui a décidé d'utiliser la solution de vote ;
- posséder si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment via Internet, d'au moins deux prestataires différents.

Le rapport d'expertise, et ses annexes doivent être remis au responsable de traitement et aux prestataires de solution de vote par correspondance électronique, notamment via Internet.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

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

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 1 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à 24 mois, qu'il est possible de prouver que l'élément sur lequel a porté cette expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 2 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à 6 mois, qu'il est possible de prouver que l'élément sur lequel a porté l'expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 3 doit être réalisée de nouveau, pour chaque élément, pour chaque élection.

L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il est tenu de prendre toutes dispositions et précautions utiles afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

Le vote

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales prévues par le code pénal.

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

Pour se connecter à distance ou sur place au système de vote, l'électeur doit s'authentifier conformément à la présente recommandation et à l'aide d'un moyen répondant à l'objectif de sécurité correspondant au niveau de risque identifié pour le scrutin. Au cours de cette procédure, le serveur de vote vérifie l'identité de l'électeur et que celui-ci est bien autorisé à voter.

Dans ce cas, il accède aux listes ou aux candidats officiellement retenus et dans l'ordre officiel.

L'électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l'écran, indépendamment de toute autre information. Il doit avoir la possibilité de revenir sur ce choix. Il valide ensuite son choix et cette opération déclenche l'envoi du bulletin de vote matérialisé vers le serveur des votes. L'électeur reçoit alors la confirmation de son vote et dispose de la possibilité de conserver trace de cette confirmation. La solution de vote par correspondance électronique, notamment via

Internet, doit proposer toutes les options offertes par les textes fondant le vote, le cas échéant le vote nul ou blanc.

Dans le cas où le scrutin est mixte, composé d'un vote par correspondance électronique associé à un vote par correspondance papier par exemple, il convient que le vote électronique permette aux électeurs les mêmes possibilités que celles offertes par le vote papier, telle que la possibilité de voter nul ou blanc lorsque cela est prévu pour un scrutin, afin de ne pas créer de distorsion en fonction du moyen utilisé. Dans le cas où ces différentes possibilités sont offertes à l'électeur, il convient d'être attentif au fait qu'une personne ne puisse pas voter deux fois, notamment en utilisant le système par correspondance papier et le système par Internet. Ainsi la solution retenue doit permettre d'écarter les votes par correspondance papier d'une personne ayant déjà voté par Internet.

Les garanties minimales pour un contrôle a posteriori

Pour des besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote par correspondance électronique, notamment via Internet, doit pouvoir fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :

- le procédé de scellement est resté intègre durant le scrutin ;
- les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls détenteurs ;
- le vote est anonyme lorsque la législation l'impose ;
- la liste d'émargement ne comprend que la liste des électeurs ayant voté ;
- l'urne dépouillée est bien celle contenant les suffrages des électeurs et qu'elle ne contient que ces suffrages ;
- aucun décompte partiel n'a pu être effectué durant le scrutin ;
- le dépouillement de l'urne peut être vérifié a posteriori et qu'il s'est déroulé de façon correcte.

La conservation des données portant sur l'opération électorale

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) doivent être conservés sous scellés jusqu'à l'épuisement des voies et délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote.

Obligation doit être faite au prestataire de service, le cas échéant, de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation de ces supports.

Lorsqu'aucune action contentieuse n'a été engagée à l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

Dispositions transitoires et finales

La présente délibération est publiée au Journal officiel de la République française. Elle devra être prise en compte par les responsables de traitement après un délai transitoire de douze mois à compter de sa publication.

La présidente,

M.-L. Denis

Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une reco...

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239>

5 sur 5 09/03/2021 à 10:43

- Fiche ISA

Annexe relative à la Sécurité des Informations

- Ci-après désignée « l'ISA » -

CETTE PAGE DOIT ÊTRE SUPPRIMÉE SI CE DOCUMENT EST INTÉGRÉ À UN CONTRAT

Version: 3.1
Version française
Date: 01 septembre 2020
Pages: 14

Contacts:

BuyIn	Marc WESSEL (marc.wessel@buyin.pro) +49 228 433 21221
DTAG	Gero Krüger (gero.kruger@telekom.de) +49 228 18133485
Orange	Valérie Mercier (valerie.mercier@orange.com) +33 6 78 59 21 35

PRINCIPES GÉNÉRAUX

La présente Annexe relative à la Sécurité des Informations (ISA) établit les exigences de sécurité IT de Deutsche Telekom AG (DTAG) et/ou Orange SA (Orange). Si l'ISA s'applique aux Livrables du contrat, le Fournisseur doit considérer ces exigences comme un standard de sécurité minimum qui doit être appliqué pendant toute la durée du Contrat, que les Livrables soient fournis par ce contrat ou un distributeur tiers.

Ces exigences couvrent différents aspects de la sécurité de l'information et certaines d'entre elles dépendent de la nature des Livrables fournis dans le cadre du Contrat.

Par ailleurs, ces exigences pourront être renforcées par des exigences complémentaires qui seront fournies par l'Acquéreur et agréées par les Parties dans un document annexé au Contrat, au NPA et/ou à la Commande.

ORDRE DE PRIORITÉ DES DOCUMENTS

La présente ISA est un document standard qui s'applique à tout Contrat conclu avec le Fournisseur qui y fait référence.

1. Le Contrat prévaut sur l'ISA sauf si un ordre de priorité différent a été établi dans le Contrat.
2. Nonobstant ce qui précède, tous les termes commençant par une majuscule ou écrits en lettres capitales seront interprétés conformément aux définitions figurant à la fin de la présente ISA, et à défaut d'une telle définition, tels qu'ils sont définis dans le Contrat contenant la référence à la présente ISA.

Les Parties conviennent que l'ISA prévaut sur les documents du Fournisseur définissant les exigences de sécurité attachés ou référencés dans le Contrat, NPA et/ou Commande.

APPLICABILITÉ GÉNÉRALE

Le Fournisseur se conformera aux exigences de l'ISA relatives aux Livrables suivants :

- **Logiciel** fait référence à un package logiciel standard du Fournisseur et/ou à un logiciel développé spécifiquement à partir d'un cahier des charges convenu par les Parties (ex. Production Logicielle);
- **Matériel** inclus tout logiciel /firmware (ex. terminaux, systèmes, équipements, etc.) ;
- **XaaS/Cloud Services** (ex. Software As A Service)
- **Services Professionnels** prestations d'installation, formation, intégration, maintenance et/ou consulting.

APPLICABILITÉ GÉNÉRALE DES SECTIONS EN FONCTION DES LIVRABLES

Les sections suivantes s'appliquent à tous les Livrables du Fournisseur :

- **Section A:** "Respect du Contrat et des standards"
- **Section B:** "Sécurité Organisationnelle"
- **Section C:** "Gestion des incidents"

Les sections ci-dessous s'appliquent en fonction de la nature des Livrables tels que définis dans la table A:

- **Section D:** "Chiffrement et authentification"
- **Section E:** "Security by design"
- **Section F:** "Gestion des correctifs de sécurité"
- **Section G:** "Données de l'Acquéreur en XaaS/Cloud Services"
- **Section H:** "Contrôle d'accès au XaaS/Cloud Services"
- **Section I:** "Opérations XaaS/Cloud Services"
- **Section J:** "Accès et utilisation des systèmes et ressources de l'Acquéreur"
- **Section K:** "Intervenants et sécurité"

Livable	Sections concernées
---------	---------------------

l'ISA

RESPECT DU STANDARDS

Table

A:

Logiciel	A, B, C, D, E, F
Matériel	A,B, C, D, E, F
XaaS/Cloud Services	A, B,C, D, E, F, G, H, I
Services Professionnels	A, B, C, J, K

Application des sections de

CONTRAT ET DES

Évaluation de la

Sécurité des Livrables

Sur demande de l'Acquéreur, le Fournisseur doit fournir sous 10 jours ouvrables toute information/documentation nécessaire pour évaluer la sécurité des Livrables : rapports de test/audit, scans de vulnérabilité et analyses de la robustesse du code source.

Politique de Sécurité

Le Fournisseur doit appliquer une politique de sécurité de l'information d'entreprise en tant qu'approche standard conformément à la norme ISO/IEC 27001 ou à toute autre norme.

Si le Fournisseur est certifié, il doit présenter sa certification de sécurité et tenir l'Acquéreur informé des renouvellements ou annulations de ses certifications.

Si le Fournisseur est sélectionné sur la base d'une certification (ex ISO/IEC 27001), le Fournisseur doit maintenir cette certification pendant toute la durée contractuelle.

Audit

L'Acquéreur et Orange SA et/ou Deutsche Telekom AG peuvent procéder à des audits afin de vérifier si le Fournisseur respecte les exigences de sécurité de l'Acquéreur et d'Orange et/ou de DTAG définies dans le Contrat

Recours à des services tiers

Dans le cas d'un recours à des services tiers dans la fourniture d'un Livrable, le Fournisseur doit s'assurer que ceux-ci sont toujours conformes aux exigences de sécurité définies dans le Contrat.

Conformité aux spécifications NESAS

NOTE: le paragraphe A.5 est seulement applicable aux équipements réseau mobile (équipement pour le cœur de réseau mobile, le RAN et l'accès).

Le Fournisseur d'équipements de réseau mobile doit évaluer le développement et le cycle de vie des équipements selon les spécifications adéquates du NESAS (Network Equipment Security Assurance Scheme), émises par la GSMA (GSMA PRD FS.13/15/16), dans la version en cours.

Le Fournisseur doit également fournir à Orange/DT les résumés des rapports d'audit associés, effectués par un organisme accrédité. L'évaluation doit être finalisée avant de fournir tout équipement réseau mobile.

Non-respect des dispositions de l'ISA

Dans le cas où le Fournisseur est informé du non-respect des exigences de sécurité dans les Livrables, le Fournisseur doit rapidement fournir à l'Acquéreur une analyse de la situation et un plan de remédiation. Si le plan de remédiation est accepté par l'Acquéreur, il est mis en œuvre par le Fournisseur sans surcoût pour l'Acquéreur et le Fournisseur doit fournir la preuve de l'efficacité du plan de remédiation.

Si le non-respect persiste ou si le plan de remédiation n'est pas accepté, cela constitue automatiquement un manquement grave au Contrat.

SÉCURITÉ ORGANISATIONELLE

Structure

Sur demande de l'Acquéreur, le Fournisseur doit fournir l'information sur son organisation de la sécurité.

Point de contact

Le Fournisseur doit nommer un point de contact responsable de la sécurité ainsi qu'un correspondant issu des instances dirigeantes ou un responsable Grands Comptes afin de traiter des problèmes faisant l'objet d'une escalade managériale et/ou signalisation. Les contacts sont identifiés pour chaque projet et toute modification doit être communiquée sans délai.

Revue de Sécurité

Une fois par an, sur demande de l'une des 2 parties, le Fournisseur et l'Acquéreur organisent une réunion visant à réaliser une revue des points de sécurité (ex. évolutions et opérations programmées qui sont susceptibles d'avoir un impact potentiel sur la sécurité).

Chaque partie peut solliciter une réunion de sécurité exceptionnelle lorsque la situation impose une analyse en commun ou une décision immédiate (par exemple : un incident majeur ou une évolution significative des menaces). Cette réunion doit être acceptée par l'autre partie.

Mesures de Sécurité pour les données de l'Acquéreur

Par données de l'acquéreur il est entendu tout bien informationnel de l'Acquéreur, c'est-à-dire les données commerciales (par exemple les contrats, les négociations, les données financières) et/ou les données techniques et SI (par exemple schémas d'architecture fonctionnelle, réseau, plans d'adressage).

Le Fournisseur doit mettre en place les mesures suivantes pour les données de l'Acquéreur qui sont classifiées comme confidentielles par l'Acquéreur, c'est-à-dire envoyées de manière chiffrée par l'Acquéreur et/ou marquées confidentiel :

- toutes ces données doivent être chiffrées lors du stockage ou du transfert de celles-ci ;
- un système d'authentification forte doit être mis en place (ex. authentification à 2 facteurs).

Les Parties doivent convenir par avance des moyens appropriés permettant, en cas de besoin, d'échanger des données chiffrées.

GESTION DES INCIDENTS

Détection

Le Fournisseur doit mettre en place les mesures pour détecter les incidents de sécurité impactant l'Acquéreur et se produisant dans l'environnement du Fournisseur. Les incidents de sécurité sont, de manière non exhaustive, la perte, la modification, la divulgation ou l'accès non autorisé aux données ou informations de l'Acquéreur et la divulgation non autorisée de code source propriétaire.

Notification

Le Fournisseur doit notifier sans délai l'Acquéreur dans le cas d'un tel incident de sécurité.

En cas de violation de la sécurité des données ou de divulgation non autorisée d'information de l'Acquéreur, le Fournisseur doit notifier l'Acquéreur conformément à la législation en vigueur, et au plus tard dans un délai de 24 heures après en avoir pris connaissance.

Les détails des incidents de sécurité doivent être conservés par le Fournisseur au moins jusqu'à la prochaine revue de sécurité entre les Parties.

Résolution

Le Fournisseur doit immédiatement résoudre les incidents de sécurité et informer l'Acquéreur de l'avancement et de la clôture de l'incident. Cette obligation est une obligation de résultat.

Suspension de l'accès aux systèmes de l'Acquéreur

NOTE: le paragraphe C.4 n'est pas applicable aux Livrables Logiciel, Matériel et aux Services XaaS/Cloud.

Dans le cas où un incident de sécurité concerne les Services Professionnels, l'Acquéreur peut suspendre l'accès à ces systèmes jusqu'à la résolution de l'incident.

Suspension de l'accès de l'Acquéreur aux Services XaaS/Cloud

NOTE: le paragraphe C.5 n'est pas applicable aux Livrables Logiciel, Matériel et aux Services Professionnels.

Dans le cas d'un incident de sécurité concernant les Services XaaS/Cloud (ex. intrusion dans le système, malware), l'Acquéreur est susceptible de suspendre son accès au service concerné jusqu'à la résolution de l'incident.

Dans le cas où l'Acquéreur ne peut lui-même suspendre l'accès, l'Acquéreur demandera explicitement au Fournisseur de suspendre tout accès de l'Acquéreur jusqu'à la résolution de l'incident. Le Fournisseur devra prendre en compte immédiatement cette demande.

Rapports de sécurité pour les Services XaaS/Cloud Services et les Services Professionnels

NOTE: le paragraphe C.6 n'est pas applicable aux Livrables Logiciel et Matériel.

À concurrence de deux fois par an, l'Acquéreur peut demander au Fournisseur un rapport de sécurité relatif aux Services XaaS/Cloud. Ce rapport de sécurité comprend, entre autres, les informations suivantes :

- le nombre d'incidents de sécurité détectés au cours des 12 derniers mois, en séparant les causes internes et externes le cas échéant ;
- les informations relatives aux incidents de sécurité au cours de la période : heure de détection, nature et impact, solution de remédiation, heure de rétablissement du service, heure de clôture de l'incident, temps de résolution.

CHIFFREMENT ET AUTHENTIFICATION

Modification des données d'authentification et des clés de chiffrement par l'Acquéreur

Toutes les données d'authentification et clés cryptographiques (ex. certificats, clés privées/publiques, clés symétriques, mots de passe ...) dans les Livrables Logiciel et Matériel doivent être modifiables par l'Acquéreur et protégées conformément à l'état de l'art. Pour les données d'authentification et les clés de chiffrement non modifiables par l'Acquéreur, Le Fournisseur doit fournir à DTAG et /ou Orange la liste exhaustive de celles-ci ainsi que leurs finalités. Pour les Services XaaS/Cloud, cette demande concerne uniquement les données d'authentification utilisées par l'Acquéreur pour protéger ses données, y compris les comptes administrateurs.

Robustesse des algorithmes de chiffrement et des clés

Le Fournisseur doit uniquement utiliser des algorithmes de chiffrement standard recommandés par les institutions gouvernementales (ex BSI, ANSSI et NIST) à la date de signature ou de renouvellement du Contrat.

SECURITY BY DESIGN - SÉCURITÉ INTÉGRÉE À LA CONCEPTION

Hardening

Le Fournisseur doit mettre en oeuvre les bonnes pratiques de durcissement des configurations (« hardening security »). Cela inclut notamment la restriction des protocoles d'accès, la suppression ou la désactivation des logiciels, ports réseau ou services non utilisés, la suppression des fichiers ou des comptes utilisateurs inutiles, la restriction des droits d'accès aux fichiers, l'installation des correctifs de sécurité, ainsi que l'activation de la journalisation.

Le Fournisseur doit produire des Livrables configurés par défaut conformément à l'état de l'art en matière de sécurité (ex. <https://www.cisecurity.org/>). Ceci s'applique également aux composants et services fournis par des tiers.

Nonobstant ce qui précède, le Fournisseur doit fournir à l'Acquéreur toutes les informations nécessaires pour configurer et utiliser les Livrables de façon sécurisée et s'assurer que ces informations sont mises à jour pendant toute la durée du Contrat.

De plus, le Fournisseur doit s'assurer que les Livrables ne contiennent pas de Backdoors.

Tests du logiciel pour les failles de sécurité

Le Fournisseur doit tester les Livrables pour s'assurer qu'ils sont exempts de vulnérabilités critiques, telles que listées dans le "Top 25 CWE/SANS" (<http://cwe.mitre.org>) et/ou "TOP 10 OWASP" (<http://www.owasp.org>) à la date de livraison (ex. robustesse de la validation des entrées face aux attaques par injection, telles que les injections SQL, comportement prédictible en cas de surcharge, etc.)

Mesures complémentaires

A la demande de l'Acquéreur, DTAG et/ou Orange, les Parties peuvent mutuellement convenir de mesures complémentaires de sécurité que les Livrables devront satisfaire.

Ces mesures complémentaires peuvent être regroupées dans un document intitulé "Security Statement of Compliance" et être intégrées au Contrat et/ou au NPA.

GESTION ET CORRECTION DES VULNÉRABILITÉS LOGICIELLES

Détection

Le Fournisseur s'engage à mettre en place un système de gestion des Vulnérabilités et des alertes permettant notamment de suivre les sources d'alertes de sécurité externes (ex. alertes émises par les éditeurs/constructeurs, CERTs ...) et se tenir informé des Vulnérabilités pouvant impacter les Livrables (y compris celles impactant les composants tiers utilisés).

CVE standard

Lorsque cela est pertinent, chaque Vulnérabilité détectée par le Fournisseur est identifiée par une CVE unique associée à un score CVSS (v3 ou supérieure), consistant en un score de base CVSS, le score temporel et le vecteur. Toute alternative à ce dispositif doit préalablement avoir fait l'objet d'une autorisation écrite de l'Acquéreur.

Notifications

Le Fournisseur doit fournir à l'Acquéreur, sans délai, les informations sur chaque Vulnérabilité (avec un score CVSS supérieur ou égal à 7.0) incluant les Zero-Day impactant les Livrables ainsi que leurs conséquences (ex. CVE, CVSS score, composants et services affectés).

Le Fournisseur doit communiquer les avis de sécurité au format cvrf/xml ou tout autre format parsable par email au cert@orange.com et/ou cert@telekom.de

Service level agreement pour la correction des Vulnérabilités

Pour chaque Vulnérabilité impactant les Livrables, le Fournisseur s'engage :

- à faire tous les efforts nécessaires pour fournir à l'Acquéreur le correctif temporaire dans les délais fixés par le tableau ci-après; et
- à fournir à l'Acquéreur le Correctif Officiel dans les délais fixés ci-après.

note CVSS base score v2	Délai maximum pour fournir un Correctif Temporaire	Délai maximum pour fournir un Correctif Officiel
7.0-10.0	5 (cinq) jours ouvrés	30 (trente) jours ouvrés
0-6.9	non applicable	6 (six) mois

Le délai court à partir de la découverte de la Vulnérabilité sauf si la Vulnérabilité est présente dans un composant d'une Tierce Partie dans ce cas le délai court à compter de la date de disponibilité du correctif.

Maintenance sécurisée des composants de Tierce Partie

Le Fournisseur doit s'assurer que les composants provenant de tiers utilisés dans les Livrables sont maintenus sécurisés pendant la période de maintenance ou de Service sous contrat avec l'Acquéreur.

Anomalie de sécurité

Le Fournisseur accepte que l'Acquéreur puisse ouvrir un ticket de maintenance pour corriger chaque Vulnérabilité impactant le Livrable et détectée par l'Acquéreur pendant la période contractuelle de maintenance et/ou de garantie. En sus de la section **Erreur ! Source du renvoi introuvable.**, le Fournisseur doit respecter les conditions de maintenance pour corriger l'anomalie associée à la Vulnérabilité.

Exceptions

Le Fournisseur s'engage à déployer des efforts commercialement raisonnables afin d'aider l'Acquéreur à corriger les Vulnérabilités :

- dans les cas requérant une réponse plus rapide que celle prévue dans le tableau ci-dessus (par exemple la publication dans la presse d'une vulnérabilité présente dans un Livrable utilisé par l'Acquéreur) et
- dans l'environnement nécessaire à l'exploitation du Livrable (par exemple le système d'exploitation d'un Livrable Logiciel)

Domage et intérêts/Pénalités

En complément des pénalités appliquées suite à une violation patente telle que visée à la section A.6 « Non-respect des dispositions de l'ISA », l'Acquéreur peut demander des pénalités au Fournisseur comme mentionné dans les sections « Dommages » ou « Pénalités » du Contrat.

Les pénalités suivantes s'appliquent en cas de Vulnérabilité :

En cas de défaillance du fournisseur à livrer un Correctif Officiel de sécurité concernant des Vulnérabilités dont la note CVSS est supérieure ou égale à 7 conformément au tableau défini dans la section **Erreur ! Source du renvoi introuvable.** « **Erreur ! Source du renvoi introuvable.** », les pénalités sont calculées de la façon suivante :

$$M = V \times N / 300$$

M : montant des pénalités.

V : V correspond à la valeur des Livrables.

N : nombre de jours civils après le délai du Correctif Officiel.

Sécurité relative à la maintenance

Pendant la durée de maintenance du contrat ou de la garantie, le Fournisseur doit fournir les Livrables Logiciel et Matériel ainsi que les nouvelles versions avec tous les correctifs de sécurité. Ces correctifs peuvent être appliqués ou fournis au même moment dans des composants/packages séparés.

Pendant le cycle de vie du Livrable, le Fournisseur doit fournir à l'Acquéreur les correctifs de sécurité dès la publication de ceux-ci, en respectant les délais de correction définis à la section **Erreur ! Source du renvoi introuvable.**

Le Fournisseur doit fournir les informations (ex CVE, CVSS score) à l'Acquéreur concernant les Vulnérabilités corrigées.

DONNÉES DE L'ACQUÉREUR DANS LES SERVICES XAAS/CLOUD

Limitation de l'utilisation des données de l'Acquéreur

Le Fournisseur ne doit utiliser, traiter, transmettre ou stocker les données de l'Acquéreur dans les Services XaaS/Cloud qu'aux fins de la fourniture du Service.

Séparation des données de l'Acquéreur

Le Fournisseur s'engage à séparer les données de l'Acquéreur des données des autres clients du Fournisseur.

Confidentialité des données de l'Acquéreur

Le Fournisseur s'engage à chiffrer toutes les données classées confidentielles par l'Acquéreur lors du transfert ou du stockage de celles-ci.

Solutions de chiffrement du Fournisseur

Dans le cas où l'Acquéreur utilise une solution de chiffrement du Fournisseur pour protéger ses données, le Fournisseur s'assure :

- que toutes les données soient chiffrées lors du stockage ou du transfert, et
- qu'un système d'authentification forte soit mis en place (ex. authentification à 2 facteurs).

Gestion des informations et des accès de l'Acquéreur

Le fournisseur s'engage à :

- journaliser les accès et actions sur les données de l'Acquéreur dans le XaaS /Service Cloud, y compris ceux de ses employés ou de tiers désignés, et
- conserver ces journaux pour la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou à défaut pour une durée maximum de 6 mois.

Les extraits des journaux conservés doivent être communiqués à l'Acquéreur sur demande de ce dernier.

Réversibilité des données de l'Acquéreur

A échéance du NPA et/ou de la commande, le Fournisseur doit restituer toutes les données de l'Acquéreur dans le XaaS/Cloud Service dans un format convenu et sur une période convenus au préalable avec l'Acquéreur.

Conformément aux sections **Erreur ! Source du renvoi introuvable.** et G.4, seules des connexions chiffrées doivent être utilisées pour la réversibilité des données de l'Acquéreur, sauf exception validée par écrit par l'Acquéreur.

A la fin de la période de réversibilité des données, le Fournisseur doit détruire tous les environnements de l'Acquéreur et les données dans le Service XaaS/Cloud Service d'une façon qui permette de s'assurer qu'elles ne peuvent être ni accédées ni lues.

Le Fournisseur doit fournir à l'Acquéreur un certificat de destruction.

CONTRÔLE D'ACCÈS DES SERVICES XAAS/CLOUD

Sécurité Physique

Le Fournisseur doit fournir des locaux sécurisés pour les infrastructures de production en Cloud et pour les sites depuis lesquels sont réalisées les opérations à distance.

Les mesures de sécurité doivent inclure à minima les éléments suivants :

- L'accès physique doit nécessiter une autorisation et être contrôlé ;
- Toute personne doit porter sur le site un badge officiel de façon visible ;
- Les visiteurs doivent signer un registre des visiteurs et être accompagnés et/ou surveillés dans les locaux ; et
- La possession des clés/cartes d'accès et la capacité d'accéder sur le site doivent être contrôlées. Le personnel du Fournisseur quittant la société doit impérativement restituer les clés/cartes .

Contrôle d'accès et gestion des mots de passe

Le Fournisseur doit contrôler l'accès aux systèmes, en restreignant ces accès aux seules personnes dûment autorisées.

Le Fournisseur doit mettre en œuvre une politique de mots de passe sur les composants de l'infrastructure et les environnements Cloud utilisés. Le Fournisseur doit protéger les mots de passe en utilisant des solutions de sécurité telles que les coffres-forts numériques.

Le Fournisseur met en place un système de contrôle et de journalisation des accès conçu pour s'assurer que seuls les personnel d'exploitation et de maintenance autorisés disposent d'accès appropriés aux systèmes. Ce système de contrôle d'accès doit comporter des mécanismes d'authentification, d'autorisation et de gestion des droits d'accès (attribution, provisionnement et révocation des droits d'accès) des employés et utilisateurs désignés par le Fournisseur.

Revue des droits d'accès

Les comptes d'accès des employés du Fournisseur au réseau et au système d'exploitation doivent être revus régulièrement pour s'assurer de la légitimité des droits d'accès.

Dans le cas où un employé du Fournisseur ne fait plus partie du projet sous contrat, le Fournisseur devra prendre rapidement les mesures nécessaires pour mettre fin aux accès associés : accès réseau, moyens téléphoniques et accès physiques.

Passerelle de sécurité

Le Fournisseur doit utiliser des passerelles de sécurité (ex. firewalls, routeurs, proxies, reverse proxies) pour contrôler l'accès Internet avec les services du Fournisseur afin de ne permettre que les flux autorisés.

Les passerelles de sécurité du Fournisseur doivent être configurées avec des politiques de sécurité et de filtrage des flux appropriés basées sur les protocoles, les ports et les adresses IP sources/destinations. Ces politiques de sécurité et de filtrage doivent donc permettre d'identifier les sources, destinations et types de flux autorisés.

Contrôles Anti-malware

Le Fournisseur doit disposer de logiciel(s) anti-malware pour scanner les fichiers téléchargés. La liste des Malware doit être mise à jour au moins une fois par jour.

Chiffrement et connexions distantes aux Services XaaS/Cloud

Pour les accès et l'utilisation des Services XaaS/Cloud Service par l'Acquéreur, seules des connexions chiffrées doivent être utilisées sauf exception acceptée par écrit par l'Acquéreur.

Le Fournisseur doit s'assurer que seules des connexions authentifiées et chiffrées sont utilisées par des tiers ayant un accès distant aux données de l'Acquéreur exploitées et stockées dans les Services XaaS/Cloud .

Dans tous les cas, les dernières versions de navigateurs doivent être supportées pour la connexion aux Services XaaS/Cloud.

OPERATIONS DE XAAS/CLOUD SERVICES

Tests de Pénétration

Le Fournisseur doit s'assurer de la sécurité des Services XaaS/Cloud Service en effectuant des tests de pénétration au moins une fois par an. Le résultat et le plan de correction de ces tests doivent être partagés avec DTAG et/ou Orange SA.

Nonobstant ce qui précède, le Fournisseur doit permettre à DTAG et/ou Orange SA de réaliser des tests de pénétration des Services XaaS/Cloud Service sur son environnement de production.

Données de Production et environnement

Le Fournisseur ne doit pas utiliser les données de production pour des activités de tests.

Le Fournisseur doit séparer les environnements de développement, de test et de production (ex. réseau, données, applications, etc.).

Plan de reprise d'activité (Disaster recovery plan)

Le Fournisseur doit définir et maintenir à jour un plan de reprise d'activité et s'assurer qu'il est testé à intervalles réguliers.

Les sauvegardes doivent être détruites de façon sécurisée par le Fournisseur lors du décommissionnement ou la mise au rebut du matériel.

Maintenance pour des besoins de sécurité

Le Fournisseur doit appliquer et tester préalablement sur un environnement de test tout patch de sécurité devant être déployé sur le Service XaaS/Cloud. C'est seulement à l'issue de tests positifs sur l'environnement de test que le Fournisseur pourra déployer le patch sur l'environnement de production.

Services rendus par des tiers

Le Fournisseur doit notifier l'Acquéreur de toute intervention prévue de services tiers (ex. data center services) dans la fourniture du Service.

Relocalisation des données

Le Fournisseur doit notifier l'Acquéreur dans le cas où les données de l'Acquéreur (y compris les données de sauvegarde) sont relocalisées vers un autre centre de données que ceux initialement convenus dans le Contrat.

ACCESS ET UTILISATION DES SYSTÈMES OU RESSOURCES DE L'ACQUÉREUR

Cette section ne s'applique que si l'Acquéreur permet au Fournisseur l'accès et l'utilisation de ses systèmes pour l'exécution du contrat.

Physique

Si l'Acquéreur fournit un accès et/ou des équipements d'interconnexion installés dans les locaux du Fournisseur, le Fournisseur s'assure que :

- le contrôle d'accès physique soit appliqué dans l'espace technique où l'équipement est installé ; et
- l'accès physique à cet équipement soit strictement limité aux seules personnes ayant besoin de cet accès aux fins d'exécution du Contrat et dûment autorisées par le Fournisseur.

Systèmes de l'Acquéreur

Le Fournisseur s'engage à :

- accéder et utiliser les systèmes de l'Acquéreur aux seules fins de la fourniture des Livrables ;
- s'assurer que les accès et le transfert de données ne sont pas utilisés pour réaliser une attaque (ex. vérification de programmes malveillants);
- respecter les moyens d'accès et les règles définies par l'Acquéreur et fournies au Fournisseur au préalable (ex. respecter le plan d'adressage réseau et les temps de réponse communiqués par l'Acquéreur);
- s'assurer que quiconque intervenant pour le compte du Fournisseur ayant besoin d'utiliser les systèmes de l'Acquéreur est dûment autorisé par le Fournisseur et que ses données d'identification ont été fournies à l'Acquéreur ;
- s'assurer que seules les ressources du Fournisseur dûment autorisées sont connectées aux systèmes de l'Acquéreur.

Ressources du Fournisseur

NOTA: Cette section est seulement applicable entre l'Acquéreur d'Orange et le Fournisseur. Pour DTAG, le Fournisseur accèdera uniquement au réseau de l'Acquéreur en utilisant la solution d'accès distant de DTAG.

Si les Ressources du Fournisseur sont utilisées pour accéder et/ou s'interconnecter avec les systèmes de l'Acquéreur, le Fournisseur s'engage à :

- suivre les bonnes pratiques de sécurité de gestion de ces Ressources (ex : maintenir les Ressources à jour avec les derniers patchs de sécurité tels que les anti-malware logiciel et des patchs des systèmes d'exploitation, configurer des privilèges restreints pour les utilisateurs, configurer la restriction des droits d'exécution depuis des supports amovibles, mettre en place des mécanismes de verrouillage de sessions sur les Ressources après une courte période d'inactivité...);
- s'assurer que les Ressources (incluant les tokens d'authentification, les mobiles et les numéros de téléphone associés) sont dédiées au Fournisseur et seulement utilisées par ses employés et tiers convenus pour fournir les Livrables ;
- mettre en place un contrôle d'accès réseau sur les Ressources du Fournisseur utilisées pour l'exécution du service ;
- mettre en place un système d'authentification forte (ex. authentification à deux facteurs) pour les accès à ces Ressources, et assurer la traçabilité de l'utilisation de ces Ressources pour tous les utilisateurs ;
- conserver ces journaux pour la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou défaut pour une durée maximum de 6 mois ;
- fournir à l'Acquéreur à sa demande un extrait des journaux conservés.

Si l'Acquéreur fournit des comptes au Fournisseur, le Fournisseur s'engage à :

- assurer la traçabilité de l'attribution et l'utilisation de ces comptes;

- conserver les traces associées pendant la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou défaut pour une durée maximum de 6 mois.; et
- fournir à l'Acquéreur à sa demande un extrait des traces conservées.

Systemes et applications de l'Acquéreur

Si l'Acquéreur fournit des comptes au Fournisseur, le Fournisseur s'engage à :

- notifier sans délai l'Acquéreur lorsqu'un compte n'est plus nécessaire et ;
- s'assurer que les comptes fournis pour des communications serveur sont utilisés pour cette seule finalité.

Management des Ressources de l'Acquéreur

Si l'Acquéreur fournit des Ressources Physiques (logiciel, matériel, ordinateur, clé USB, badge, tablette, smartphone, accès ou équipement d'interconnexion ...) au Fournisseur, celui-ci doit surveiller et contrôler étroitement l'utilisation de ces Ressources. A la fin du contrat, le Fournisseur s'engage à restituer les Ressources de l'Acquéreur encore en sa possession.

SERVICES PROFESSIONNELS ET SÉCURITÉ

Sensibilisation et Formation

Le Fournisseur doit s'assurer que ses employés ainsi que les tiers participant à la fourniture des Livrables :

- possèdent les compétences de sécurité appropriées (e.x pour gérer les incidents de sécurité); et
- connaissent le contenu et la mise en œuvre des règles de sécurité.

Les règles de sécurité spécifiques à l'Acquéreur

Si l'Acquéreur fournit des règles spécifiques de sécurité pour réaliser les Services Professionnels, le Fournisseur doit s'assurer que ses employés et tous les tiers sont informés des règles avant le démarrage des activités.

Sous-Traitants

Si le Fournisseur fait appel à des sous-traitants pour réaliser le contrat de l'Acquéreur, le Fournisseur doit spécifiquement les identifier comme des sous-traitants et s'assurer de la mise en œuvre des mesures appropriées nécessaires au respect des exigences du présent document .

Traitement des Livrables sensibles

Sur demande particulière de l'Acquéreur et en accord avec le Contrat, le Fournisseur s'engage à employer uniquement du personnel ayant fait l'objet d'une procédure de vérification (ex. vérifications par les autorités nationales), pour traiter des Livrables sensibles, et ce aussi bien avant le déploiement que durant toute la phase opérationnelle de maintenance.

DÉFINITIONS ET ABRÉVIATIONS

Contrat	désigne tout contrat signé par BuyIn, DTAG et/ou Orange avec le Fournisseur et contenant la référence à la présente ISA.
Actifs	désigne, conformément à la norme ISO/IEC 27005, les actifs primaires et actifs supports.
Backdoor	désigne une fonctionnalité ou un défaut d'un Livrable permettant un accès non autorisé discret/furtif aux données.

CVE	signifie « Common Vulnerabilities and Exposures » tel que défini sur le site http://cve.mitre.org/index.html .
CVSS	signifie « Common Vulnerability Scoring System » tel que défini sur le site http://www.first.org/cvss/ .
Anomalie	désigne toute déviation de la qualité réelle du Livrable au regard de la qualité convenue contractuellement (ex. défaut, non-conformité des Livrables au regard des spécifications, défaut d'exécution conforme à la documentation associée).
Livrables	désigne tout équipement, produit et/ou service commandé sur la base du Contrat principal, y compris toutes les obligations majeures et accessoires.
Sécurité des informations	désigne, conformément aux normes ISO/IEC 27001 et ISO/IEC 27005, la sécurité dans le cadre du traitement des informations et des activités (actifs primaires) reposant sur des ressources techniques (y compris, entre autres, des technologies de l'information, des locaux, des installations et des réseaux) et non techniques (y compris, de façon non limitative, des actifs supports tels que du personnel, des partenaires, des organisations, des procédures et des conditions générales).
NPA	désigne un contrat conclu par une Société Affiliée de DTAG ou Orange dans le cadre d'un Accord-cadre de BuyIn, DTAG ou Orange, selon le cas, conclu par BuyIn. NPA correspond aux termes « Accord d'exécution », « Accord Propre au Projet » et « Accord du Projet » : toute disposition utilisant le terme « NPA » s'appliquera à ce type d'accords également.
Correctif Officiel	désigne une solution mise à disposition par le Fournisseur pour corriger complètement une Vulnérabilité, par un patch officiel ou une mise à jour.
Commande	désigne un bon de commande émis par l'Acquéreur. « Commande » correspond au terme « Bon de Commande » dans les Accords conclus par DTAG et ses Sociétés Affiliées. Toute disposition utilisant le terme « Commande » s'appliquera de la même façon à « Bon de Commande ».
Acquéreur	désigne la Société Affiliée DTAG ou Orange en tant que partie au NPA ou à la Commande. « Acquéreur » correspond au terme « Partie Passant une Commande » dans les Accords conclus par DTAG et/ou Orange et ses Sociétés Affiliées. Toute disposition établie à l'égard de l'Acquéreur dans la présente ISA s'appliquera de la même façon à la « Partie émettant une Commande ».
Réseau de l'Acquéreur	désigne le réseau géré par l'Acquéreur ainsi que toutes les infrastructures d'accès réseaux nécessaires pour les communications entre les Ressources de chacune des parties.
Ressources de l'Acquéreur	désigne les matériels, logiciels et/ou services appartenant à l'Acquéreur utilisés pour la fourniture des Livrables.
Production logicielle	désigne un logiciel : (i) s'appuyant principalement et/ou étant réalisé sur la base des exigences de DTAG et/ou Orange, et/ou les spécifications fournies par ou exclusivement pour l'Acquéreur, et/ou (ii) développé ou mis en oeuvre par le Fournisseur dans le cadre de ce Contrat (et/ou tout amendement ultérieur), et/ou tout TSA et/ou tout NPA et/ou toute Commande, et qui n'a pas d'antériorité. que celui-ci soit ou non protégé par des droits de propriétés intellectuelles, de même que tous les produits ou procédés résultant de celui-ci.
Statement of Compliance	désigne une annexe au Contrat décrivant les exigences de sécurité technique détaillées sur les Livrables.
Cahier des charges	désigne un document définissant les activités, Livrables et jalons d'un projet pour la fourniture de Livrables et/ou services par le Fournisseur à l'Acquéreur.
Ressources du Fournisseur	désigne les matériels, logiciels et/ou services appartenant au Fournisseur utilisés pour la fourniture des Livrables.

Correctif Temporaire	désigne un correctif mis à disposition du Fournisseur permettant de corriger temporairement une Vulnérabilité (ex. correctifs, outils ou solutions de contournement temporaires)
Vulnérabilité	désigne une faiblesse impactant la disponibilité, l'intégrité ou la confidentialité.
XaaS	désigne le modèle de fourniture en tant que service, incluant le SaaS (Software as a Service), le PaaS (Platform as a Service), le IaaS (Infrastructure as a Service) ou équivalent.
Zero-Day	désigne une Vulnérabilité non divulguée que des hackers peuvent exploiter pour porter atteinte à la sécurité des Livrables. La Vulnérabilité est dénommée "zero-day" (ou "zero-hour", ou "0-day" ou "day zero") parce que celle-ci n'a pas été publiquement signalée ou communiquée avant d'être utilisée, laissant le Fournisseur sans délai pour développer des correctifs ou proposer des solutions permettant de réduire l'impact.

- fin du document -