

Accord-cadre

Migration du progiciel de gestion budgétaire et comptable Oracle E-Business Suite et des bases de données Oracle

PALAIS DU LUXEMBOURG ET DÉPENDANCES

CCTP

Cahier des clauses techniques particulières

Juillet 2026



ARTICLE 1. - Objet du marché	3
ARTICLE 2. - Objectifs	3
ARTICLE 3. - Contexte général de déroulement de la prestation	3
3.1. Contexte du Sénat.....	3
3.2. Contexte de la Direction des systèmes d'information.....	4
3.3. Contexte fonctionnel.....	4
ARTICLE 4. - Description de l'existant – Contexte technique d'Oracle E-Business Suite	6
4.1. Architecture applicative actuelle	6
4.2. Infrastructure technique.....	7
4.3. Bases de données.....	9
4.4. Interfaces et flux	9
ARTICLE 5. - Obligations du titulaire – Description générale.....	11
ARTICLE 6. - Description des prestations attendues (prestations forfaitaires)	12
6.1. Périmètre des prestations.....	12
6.2. Prestation de cadrage et d'audit technique.....	13
6.3. Prestations de préparation des environnements et de migration de l'application et des bases de données.....	13
6.4. Prestations de documentation et de réalisation d'un clonage	13
6.5. Prestation d'installation d'Enterprise Command Center (ECC)	14
6.6. Prestation d'installation d'Oracle APEX.....	14
6.7. Prestation de recette technique	14
6.8. Prestation de mise en production	15
6.9. Vérifications d'aptitude globale et de service régulier	15
6.10. Délais de réalisation des prestations	16
ARTICLE 7. - Description des prestations attendues (prestations sur bons de commande).....	16
7.1. Prestation d'assistance technique complémentaire post-migration.....	16
7.2. Prestation de formation.....	16
7.3. Ateliers de co-développement sur Oracle APEX	17
ARTICLE 8. - Compétences techniques attendues	17
ARTICLE 9. - Lieu d'exécution des prestations	17
ARTICLE 10. -Comitologie.....	17
10.1. Comité technique hebdomadaire.....	17
10.2. Comité de pilotage	18
ARTICLE 11. - Principes de sécurité et données personnelles.....	18
ARTICLE 12. - Réversibilité et transfert de compétences	18

ARTICLE 1. - Objet du marché

Le présent marché a pour objet :

- la réalisation d'une migration technique de l'application Oracle E-Business Suite, actuellement exploitée en version 12.2.10 vers une version cible 12.2.15 ou supérieure certifiée par l'éditeur, et des bases de données Oracle associées, depuis la version Oracle Database 12 vers une version cible Oracle Database 23 ou supérieure certifiée par l'éditeur, vers les nouveaux serveurs physiques mis à disposition par le Sénat ;
- ainsi que l'installation de la couche applicative Enterprise Command Center et de la plateforme Oracle APEX.

ARTICLE 2. - Objectifs

Les principaux objectifs poursuivis dans le cadre de ce projet sont :

- d'améliorer la sécurité et la maintenabilité du système d'information budgétaire et comptable du Sénat ;
- de garantir tout au long du projet la continuité du service pour les utilisateurs et de limiter le temps d'indisponibilité en production.
- et d'exploiter les fonctionnalités offertes par les nouvelles versions d'Oracle E-Business Suite et Oracle Database, dont la possibilité d'installer et d'utiliser les composants Oracle Enterprise Command Center et la plateforme Oracle APEX..

ARTICLE 3. - Contexte général de déroulement de la prestation

3.1. Contexte du Sénat

Le Sénat est une assemblée parlementaire constitutionnelle, qui assure notamment, en application de l'article 24 de la Constitution, la représentation des collectivités territoriales de la République. Le Sénat est composé de 348 Sénateurs.

Parmi les Sénateurs, trois Questeurs sont élus en même temps que les autres membres du Bureau du Sénat (Président du Sénat, 8 vice-présidents et 14 secrétaires du Sénat). Ils forment le Conseil de Questure, chargé de la direction de l'administration du Sénat, sous le contrôle du Bureau.

En pratique, les Questeurs gèrent tous les aspects administratifs de la vie du Sénat et disposent d'un pouvoir financier, réglementaire et de nomination, exercé le cas échéant conjointement avec le Président du Sénat.

L'administration du Sénat contribue à l'exercice des missions institutionnelles du Sénat et à la gestion de ses ressources et de ses moyens. D'une manière générale, les informations relatives au Sénat sont disponibles sur le site internet du Sénat sous la rubrique « Connaître le Sénat » (<http://www.senat.fr/role/index.html>).

L'administration du Sénat est dirigée par le Secrétaire général du Sénat, assisté d'un directeur général des missions institutionnelles, et le Secrétaire général de la Questure, assisté d'un directeur général des ressources et moyens. Les directions sont soit rattachées à la direction générale des missions institutionnelles soit rattachées à la direction générale des ressources et des moyens. Environ 1200 fonctionnaires et contractuels composent l'administration du Sénat, qui est au service des Sénatrices et Sénateurs. L'organigramme du Sénat figure en annexe n° 1.

3.2. Contexte de la Direction des systèmes d'information

La Direction des systèmes d'information (DSI) constitue l'une des 8 directions gérant les ressources et moyens du Sénat.

La DSI comprend près de 60 personnes (personnels administratifs et techniques), essentiellement répartis en trois divisions, en sus du responsable de la sécurité des systèmes d'information (RSSI) et du délégué à la protection des données (DPD) :

- une division « systèmes » en charge de l'infrastructure du système d'information du Sénat (serveurs, postes de travail, réseau) ;
- une division « applications de gestion » en charge des applications informatiques de gestion ;
- une division « applications documentaires » en charge des applications législatives et documentaires du Sénat.

L'organigramme de la DSI figure en annexe n° 2.

3.3. Contexte fonctionnel

3.3.1. L'organisation budgétaire et comptable du Sénat

3.3.1.1. Principes généraux

Le Sénat jouit de l'autonomie financière en application du principe de séparation des pouvoirs mis en œuvre par l'article 7 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires. Cette autonomie porte à la fois sur l'adoption et l'exécution du budget, l'établissement et la tenue des comptes, ainsi que leur contrôle.

Le budget du Sénat est inscrit en loi de finances dans la mission « Pouvoirs publics ». Les ressources du budget proviennent essentiellement de la dotation de l'État. En 2026, le budget du Sénat s'élève à 382,3 millions d'euros.

Le Conseil de Questure détermine le budget du Sénat. L'un des Questeurs a, par roulement pour une période trimestrielle, la qualité de Questeur délégué. À ce titre, il est l'ordonnateur des dépenses et sa signature est indispensable pour assurer leur paiement. Il est signataire des actes de nature contractuelle et des courriers adressés par le Conseil de Questure.

Les règles générales relatives à l'emploi des crédits sont établies dans le Règlement général budgétaire et comptable (RBDC) du Sénat. Conformément à ce règlement, aucune dépense ne peut être engagée par les Directeurs sans autorisation préalable du Conseil de Questure, sous réserve de l'existence de délégation et subdélégation au profit du Secrétaire Général de la Questure ou des Directeurs eux-mêmes pour les dépenses les moins importantes.

En dépenses, le budget comporte pour chacune des trois entités (Sénat, Jardin et Musée du Luxembourg) une section d'investissement et une section de fonctionnement. Chacune de ces sections se subdivise en comptes et sous-comptes.

Depuis 2013, les comptes agrégés du Sénat sont certifiés par la Cour des comptes. La Commission spéciale chargée du contrôle des comptes et de l'évaluation interne, composée de Sénateurs, donne quitus de la régularité de sa gestion au Trésorier.

3.3.1.2. Une organisation déconcentrée

Le Sénat présente la particularité de disposer d'une organisation comptable déconcentrée : l'entité comptable du Sénat comporte 14 entités budgétaires comprenant 12 des 13 directions du Sénat, la division de la Questure, des Affaires juridiques et du Contrôle interne (DQAJCI) et la Présidence.

Ces entités disposent de gestionnaires budgétaires et comptables chargés de gérer leurs budgets, de préparer les marchés publics de leurs directions (qu'ils soient autorisés par les Questeurs ou, par délégation, par les directeurs), de traiter et de mandater les factures, de suivre l'exécution budgétaire, en lien avec la division du budget et de la paie de la Direction des affaires financières et sociales (DAFS) et l'Agence comptable. De même, la relation avec les fournisseurs (commandes et achats) est décentralisée dans chaque direction disposant d'un budget.

Chaque entité budgétaire (direction) dispose d'un nombre de comptes comptables à sa disposition. En début d'année, chaque direction identifie ses dépenses et crée des engagements comptables (EC).

Le fonctionnement financier, comptable et budgétaire du Sénat est coordonné par la Direction des Affaires financières et sociales (DAFS). Elle est composée de plusieurs divisions dont notamment la division du budget et de la paie, qui assure la coordination en matière de budget et de comptabilité, et l'Agence comptable, dirigée par le Trésorier du Sénat, qui assure les contrôles avant paiements et établit les états financiers.

3.3.2. Les utilisateurs d'Oracle E-Business Suite

Depuis 2002, la gestion comptable du Sénat repose sur le **progiciel Oracle E-Business Suite**, désigné en interne sous le nom de COMPTA.

Conformément à l'organisation présentée précédemment, les principaux utilisateurs d'Oracle E-Business Suite appartiennent à la DAFS ou à l'une des directions dépensières du Sénat. La DQAJCI, qui assure un contrôle sur l'ensemble des marchés publics, valide quant à elle les déclarations informatisées d'attribution de marchés dans la solution Oracle E-Business Suite.

Seuls les utilisateurs appartenant à la DAFS, chargés de l'élaboration et du suivi du budget, d'une part, et ceux chargés du contrôle et du paiement, d'autre part, ont accès à l'ensemble des données comptables.

Tous les autres utilisateurs ont une vue partielle du système, limitée aux données de leur direction.

Au total, **120 utilisateurs ont accès à OEBS en consultation ou en modification.**

Par ailleurs, il existe un certain nombre de régies (buvettes, directions) qui font l'objet d'une comptabilité tierce dans d'autres outils qu'Oracle E-Business Suite : EBP COMPTA Pro ou SAGE 100 (hors périmètre du présent marché).

ARTICLE 4. - Description de l'existant – Contexte technique d'Oracle E-Business Suite

4.1. Architecture applicative actuelle

• Version d'Oracle E-Business Suite

La solution budgétaire et comptable du Sénat repose actuellement sur la **version 12.2.10 d'Oracle E-Business Suite**. La dernière mise à jour du progiciel a été réalisée en octobre 2021, de la version 12.2.6 à la version 12.2.10.

• Modules utilisés

Oracle E-Business Suite est utilisé pour toute la chaîne comptable du Sénat et les processus associés (mandatement, engagements comptables, comptabilisation, comptabilité analytique, immobilisations, gestion des factures et commandes, etc.).

Pour ce faire, les modules d'Oracle E-Business Suite mis en œuvre au Sénat sont les suivants :

PO	uniquement l'entité Sénat	PO (Purchase Order - Bons de commande) : gestion des engagements juridiques, achats et approvisionnements
AP	toutes les entités	AP (Account Payables - Fournisseurs) : permet de gérer les factures, le mandatement, les fournisseurs, de comptabiliser les opérations d'achat et de règlements
AR	toutes les entités	AR (Account Receivable - Recettes) : permet de gérer les factures, le mandatement, les clients, de comptabiliser les opérations de ventes ainsi que les encaissements
GL	toutes les entités	GL (General Ledger - Comptabilité générale) : permet de centraliser les écritures comptables, analytiques et budgétaires en recevant les écritures synthétiques des autres modules dits auxiliaires, qui contiennent le détail des opérations
CM	toutes les entités	CM (Cash Management – Gestion de trésorerie) : permet de gérer la trésorerie, le référentiel des banques et agences et les comptes bancaires
FA	uniquement l'entité Sénat	(Fixed Assets - Immobilisations) : permet de gérer les immobilisations et de les centraliser ;
OPSFI	uniquement l'entité Sénat	(Oracle Public Sector Financials International) : correspond à la gestion d'une « surcouche » spécifique pour le secteur public) – mandatement, engagements comptables et la sécurité des auxiliaires (SLS).
SLA	toutes les entités	(Subledger Accounting) : moteur de traduction comptable (passage des comptabilités auxiliaires PO/AP/AR et du module FA à la comptabilité générale).

• Environnements

Six environnements sont actuellement utilisés :

- Production (PROD) ;
- Développement (DEVT) ;
- Recette (RECT) ;
- Patchs (PATC) ;
- Qualification (QUAL) ;
- Versionning (VERS).

Chaque environnement est hébergé sur une même machine, regroupant l'applicatif et la base de données, localisés dans un *filesystem* dédié.

• Langues

Deux langues sont déployées : US et F

• Environnement des postes clients

Les postes clients sont en Windows 11.

Le réseau est de type LAN. Les utilisateurs peuvent y avoir également accès via un VPN (Global Protect).

La version du JRE JAVA utilisée est la Java 8 update 281.

4.2. Infrastructure technique

4.2.1. Infrastructure actuelle

Les six environnements d'Oracle E-Business Suite sont installés sur **quatre machines serveurs physiques**. En fonctionnement normal, la répartition est la suivante :

- Serveur 1 : PROD (primaire) ;
- Serveur 2 : PROD (standby) + RECT + DEVT + PATC (éteint)
- Serveur 3 : QUAL
- Serveur 4 : VERS

Les **caractéristiques** des serveurs primaires et secondaires utilisés sont les suivantes :

- ProLiant DL360p Gen8
- Bi-Processeur Inte Xeon E5-2620 6 cœurs
- 64 Go RAM
- Red Hat Enterprise Edition 6.6

Les serveurs sont sauvegardés quotidiennement en utilisant l'infrastructure de sauvegarde Dell Networker du Sénat. Par ailleurs la base de données de production est répliquée en

continue *via* Dataguard vers la base *standby*. La partie applicative de production est copiée quotidiennement par synchronisation du *filesystem* correspondant vers le serveur 2.

4.2.2. Infrastructure cible mise à disposition

Le Sénat souhaite remplacer les quatre serveurs actuels, devenus obsolètes, par trois nouveaux serveurs. Le Sénat a commandé ces serveurs en avril 2026, en anticipation du projet de migration, compte tenu des difficultés actuelles d’approvisionnement et les a reçus en juin 2026.

Le titulaire devra intégrer ces équipements, mis à la sa disposition par le Sénat, dans sa stratégie de migration.

Caractéristiques des nouveaux serveurs mis à disposition

Nombre de serveurs	3
Constructeur	Lenovo
Modèle	Lenovo ThinkSystem SR630 V4
CPU	2 x Intel Xeon 6507P 8c 3,5Ghz
RAM	128 Go
Stockage	5,3 To SSD en RAID 5
Réseau	4 x 10G Base-T
OS Cible	Red Hat Entreprise Linux 8

Le premier serveur sera dédié à la production. Le second hébergera la base Oracle *standby* de la production et une copie de l’arborescence applicative. Les autres environnements seront répartis entre les serveurs 2 et 3.

Chaque environnement est situé dans son propre *filesystem* et contient la base de données et l’applicatif.

Cette infrastructure composée de serveurs plus récents et plus puissants doit permettre d’envisager la mise en place d’une redondance, avec une possibilité de bascule du serveur de production vers sa copie en cas de défaillance du premier.

La DSI du Sénat réalisera l’installation et la configuration technique des trois serveurs, ainsi que l’installation des systèmes d’exploitation (OS) avant le processus de migration.

4.3. Bases de données

Les bases de données actuellement utilisées sont des **bases Oracle 12.1.0.2**.

Au 1^{er} mai 2026, la volumétrie de la base de données de production est d'environ 300 GO pour Oracle E-Business Suite. La volumétrie des bases des autres environnements est similaire (un clonage régulier est opéré entre les environnements PROD, QUAL et RECT).

4.4. Interfaces et flux

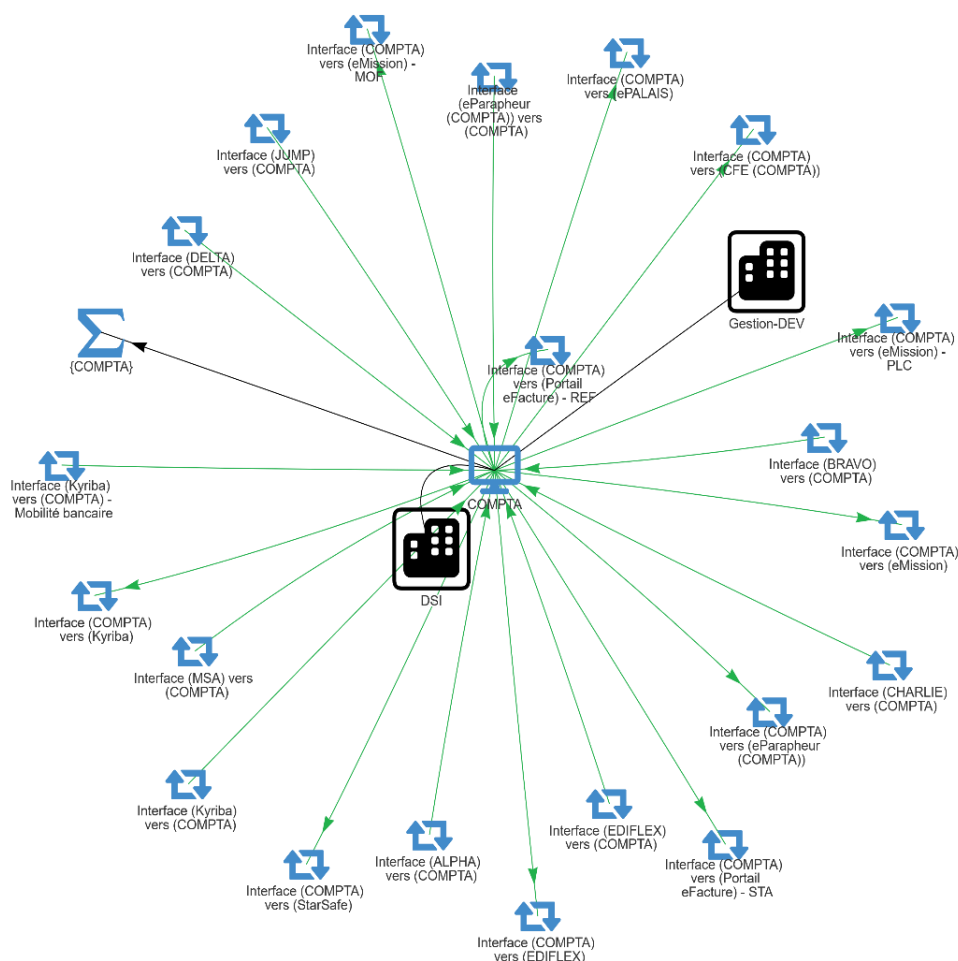
Oracle E-Business joue un rôle central dans le système d'information de gestion du Sénat et est interfacé avec 17 autres applications du Sénat, de nature diverse. Il s'agit d'applications développées en interne (IBOU, E-Mission), de processus modalisés sous BONITA, de progiciels maintenus en interne (COGNOS) ou encore de progiciels hébergés en Saas avec lesquels le Sénat échange régulièrement des fichiers (portail de facturation, EDIFLEX).

Tableau n° 1 : Liste des applications interfacées avec Oracle E-Business Suite

Nom interne	Progiciel application interne	Objet	Hébergement	Interfaces avec la solution OEBS
IBOU	Développement interne en JAVA	Suivi budgétaire	Sénat	Oui
Cognos	Progiciel IBM	Reporting	Sénat	Oui
ALPHA	Développement interne sur BONITA	Création de tiers	Sénat	Oui
BRAVO	Développement interne sur BONITA	Nouveau marché public	Sénat	Oui
CHARLIE	Développement interne sur BONITA	Sous-traitance marché public (DC4)	Sénat	Oui
DELTA	Développement interne sur BONITA	Avenant marché public	Sénat	Oui

ECHO	Développement interne sur BONITA	Service fait	Sénat	Oui
EDIFLEX	Progiciel	Marchés de travaux	Saas	Oui via SFTP
Parapheur électronique	Progiciel	Flux mandatement	Saas	Oui via SFTP
Coffre fort électronique de la chaîne comptable Docaposte	Progiciel	Factures	Saas	Oui via SFTP
Portail Docaposte eFacture	Progiciel	Factures	Saas	Oui via SFTP
E-mission	Développement interne en C++	Suivi des missions	Sénat	Oui
E-Palais	Progiciel	Fournisseurs et marchés	Sénat	Oui
Phileas	Développement interne en C++	Frais de transport	Sénat	Oui
Sirpas	Progiciel	Paie (RIB et adresses)		Oui
KYRIBA	Progiciel	Mobilité bancaire	Saas	Oui via SFTP
Sage 100	Progiciel	Commandes et fichiers SEPA	Sénat	Oui

Schéma n° 1 : principales interfaces entrantes et sortantes avec Oracle E-Business Suite (COMPTA)



ARTICLE 5. - Obligations du titulaire – Description générale

Le titulaire est tenu de mettre en œuvre dans le cadre des missions qui lui sont confiées tous procédés et moyens lui permettant de réaliser les prestations.

Le titulaire s’engage à exécuter les prestations avec tout le soin possible en usage dans sa profession.

Le titulaire s’engage à mettre à disposition des ressources ayant un niveau de connaissances et de compétence tel que définies à l’article 8 du présent CCTP.

Le titulaire est tenu à une obligation générale de conseil, d’information et d’alerte pendant toute la durée d’exécution du marché. Il informe sans délai, par écrit, le Sénat de toute difficulté, risque, contrainte technique, incohérence ou omission constatée dans le cadre de l’exécution du marché. Il propose les mesures correctives ou compensatoires qu’il estime nécessaires.

Le titulaire désigne un interlocuteur unique qui est le correspondant du Sénat et qui, à ce titre, est habilité à contrôler le respect des exigences énoncées dans le marché.

Le titulaire s'engage à prendre connaissance de l'ensemble des documents transmis par le Sénat afin de proposer un conseil et un accompagnement approprié.

Le titulaire remet les différents livrables des prestations attendues.

ARTICLE 6. - Description des prestations attendues (prestations forfaitaires)

6.1. Périmètre des prestations

Le titulaire prend en charge l'ensemble des prestations nécessaires à la réalisation de la migration de l'application Oracle E-Business Suite et des bases de données Oracle vers les dernières versions certifiées et recommandées par l'éditeur.

Le marché comprend notamment :

- l'analyse de l'existant ;
- la définition de l'architecture cible, en accord avec les prescriptions initiales du Sénat ;
- l'établissement du déroulé de mise à jour ;
- la préparation des environnements ;
- les opérations de migration de l'application et des bases de données ;
- l'établissement de la procédure de clonage ;
- la réalisation d'un clonage ;
- les tests techniques ;
- la mise en production ;
- la documentation de l'ensemble des opérations réalisées ;
- et le transfert de compétences.

Le marché comprend également l'installation des deux composants applicatifs suivants :

- Oracle Enterprise Command Center (ECC)
- Oracle APEX.

Les livrables impérativement attendus de la part du titulaire sont :

- l'audit technique de l'existant et l'étude de cadrage intégrant le plan et le planning de migration ;
- le document d'exploitation détaillant les procédures de patches et de clonage. Ce document doit être validé par le Sénat avant son adoption.

Les opérations suivantes se situent en-dehors du périmètre du présent marché :

- l'installation et l'intégration des nouveaux serveurs dans l'infrastructure du système d'information du Sénat, qui seront effectuées en amont par la DSI du Sénat ;
- la mise à niveau des développements spécifiques et des interfaces, à la charge de la DSI du Sénat ;
- la recette fonctionnelle de l'applicatif et des interfaces, réalisée par la DSI et la DAFS du Sénat.

6.2. Prestation de cadrage et d'audit technique

Lors d'une phase de cadrage, le titulaire réalise un audit technique de l'architecture actuelle d'Oracle E-Business Suite et des bases de données afin :

- de définir les versions cibles de l'applicatif Oracle E-Business Suite et d'Oracle Database retenues dans le cadre du projet de migration ;
- d'identifier les prérequis techniques de migration ;
- d'évaluer les dépendances applicatives et techniques ;
- et de définir la stratégie de migration, en précisant l'ordre des différentes étapes et le déroulé des mises à jour.

Le titulaire identifie lors de cette phase les risques techniques, les incompatibilités éventuelles et les impacts sur les applications interfacées.

À l'issue de cette phase, le titulaire fournit un document de cadrage comprenant a minima :

- un rapport d'audit de l'existant ;
- un dossier d'architecture cible ;
- un plan de migration détaillé ;
- un plan de bascule ;
- une analyse des risques ;
- et un planning détaillé.

6.3. Prestations de préparation des environnements et de migration de l'application et des bases de données

Le titulaire prépare les environnements et réalise les opérations de migration de l'application Oracle E-Business Suite et des bases de données, conformément au plan de migration et à la méthodologie agréés entre les parties lors de la phase de cadrage.

S'agissant de l'application Oracle E-Business Suite, le titulaire effectue l'ensemble des prestations nécessaires à la migration de la version 12.2.10 vers une version cible 12.2.15 ou supérieure recommandée et certifiée par l'éditeur, dont l'application des patches recommandés les plus récents et la mise à jour des composants techniques.

Le titulaire garantit l'intégrité des données, la continuité fonctionnelle et la compatibilité des modules.

Le titulaire réalise l'ensemble des prestations nécessaires à la migration des bases de données Oracle Database 12 vers Oracle Database 23 ou une version supérieure recommandée et certifiée par l'éditeur.

Le titulaire documente, à l'attention de la DSI du Sénat, l'ensemble des opérations réalisées.

6.4. Prestations de documentation et de réalisation d'un clonage

Le titulaire établit et documente une procédure complète de clonage des environnements Oracle E-Business Suite et des bases de données Oracle associées.

Cette procédure devra permettre la reproduction à l'identique d'un environnement à partir de l'environnement de référence désigné.

Après validation de la procédure par le Sénat, le titulaire réalise un clonage complet des environnements désignés.

6.5. Prestation d'installation d'Enterprise Command Center (ECC)

Le titulaire réalise l'installation d'Enterprise Command Center (ECC) sur l'application Oracle E-Business Suite dans la version supérieure recommandée et certifiée par l'éditeur.

Les prestations comprennent notamment :

- l'installation de ECC Framework ;
- l'installation du server Weblogic ;
- l'installation des patches nécessaires pour les modules demandés ;
- l'intégration d'ECC dans Oracle E-Business Suite.

Les prestations sont réalisées sur la base des licences Oracle actuellement détenues par le Sénat. Le titulaire signalera sans délai toute contrainte technique ou fonctionnelle susceptible de nécessiter l'acquisition de licences complémentaires.

6.6. Prestation d'installation d'Oracle APEX

Le titulaire réalise l'installation d'Oracle APEX sur l'application Oracle E-Business Suite. Les prestations comprennent notamment :

- l'installation d'Oracle APEX 24.1 ou supérieur ;
- l'installation d'Oracle REST Data Services (ORDS) 24.3 ou supérieur ;
- la création d'un schéma spécifique et d'un espace de travail (*workspace*) associé.

Le titulaire s'assure au préalable de la compatibilité entre les versions d'Oracle APEX et ORDS installées avec l'infrastructure cible (Red Hat Enterprise Linux 8).

Les prestations sont réalisées sur la base des licences Oracle actuellement détenues par le Sénat. Le titulaire signalera sans délai toute contrainte technique ou fonctionnelle susceptible de nécessiter l'acquisition de licences complémentaires.

6.7. Prestation de recette technique

Le titulaire réalise l'ensemble des tests techniques nécessaires à la vérification de la bonne réalisation des prestations énumérées précédemment.

Les tests comprennent notamment :

- les tests d'installation ;
- les tests de bon fonctionnement (démarrage et arrêt) ;
- les tests de performance ;
- les tests de sauvegarde et restauration ;
- les tests de reprise ;
- les tests de sécurité.

La DSI du Sénat réalise la vérification de la recette technique effectuée par le prestataire. Elle est responsable de la recette technique des interfaces.

Le titulaire fournit un rapport détaillé de recette technique.

6.8. Prestation de mise en production

Le titulaire accompagne la mise en production. Le passage en production sera exécuté dès que le Sénat aura constaté le bon fonctionnement du nouvel environnement sur le serveur de qualification.

Les prestations comprennent notamment :

- la préparation du plan de bascule ;
- la réalisation des opérations de migration en production ;
- les vérifications post-migration ;
- l'assistance au démarrage ;
- le support après la mise en production, dont la correction des anomalies imputables à la migration.

Le titulaire documente, à l'attention de la DSI du Sénat, la méthodologie de passage du serveur de développement vers le serveur de production.

6.9. Vérifications d'aptitude globale et de service régulier

6.9.1. Vérification d'aptitude globale

À l'issue des opérations de migration et préalablement à la mise en production, le Sénat procède à la vérification d'aptitude globale (Vérification de Service d'Aptitude, VSA), sur la base des éléments fournis par le titulaire.

La vérification d'aptitude globale a pour objet de vérifier que les prestations réalisées sont conformes aux exigences contractuelles et que les environnements migrés sont aptes à être exploités en production. Elle comprend notamment la vérification du bon fonctionnement des composants Oracle E-Business Suite, des bases de données Oracle migrées, des composants Enterprise Command Center et APEX, la vérification de la reprise des données et des procédures d'exploitation, de sauvegarde et de restauration.

La vérification d'aptitude est déclarée satisfaisante lorsque :

- aucune anomalie bloquante n'est constatée ;
- aucune anomalie majeure ne fait obstacle à l'exploitation de la solution ;
- les anomalies mineures font l'objet d'un plan de correction validé par le pouvoir adjudicateur.

Le Sénat prononce la vérification d'aptitude globale, la prononce avec réserves ou la refuse.

6.9.2. Vérification de service régulier

La vérification de service régulier débute à compter de la mise en production de la solution migrée et des bases de données.

La durée de la vérification de service régulier est fixée à trente jours.

La vérification de service régulier a pour objet de vérifier le fonctionnement régulier, stable et conforme de la solution et des bases de données dans les conditions réelles d'exploitation.

Pendant la période de vérification de service régulier, le titulaire assure le suivi et corrige, à ses frais, toute anomalie imputable aux prestations réalisées dans le cadre du présent marché.

La vérification de service régulier est déclarée satisfaisante lorsque, pendant toute sa durée :

- aucun incident bloquant imputable aux prestations du titulaire n'est constaté ;

- aucune anomalie majeure imputable aux prestations du titulaire n'est demeurée non corrigée au-delà du délai contractuel de correction ;
- les réserves éventuellement émises lors de la vérification d'aptitude ont été levées.

Toute anomalie bloquante imputable au titulaire interrompt la durée de la vérification de service régulier. Une nouvelle période complète de vérification de service régulier débute à compter de la correction de l'anomalie et de sa validation par le Sénat.

6.10. Délais de réalisation des prestations

Le marché s'exécute à compter de sa notification prévue en octobre 2026.

Le marché est conclu pour une durée prévisionnelle de quinze mois.

L'objectif du Sénat est d'opérer la mise en production six à huit mois après le démarrage du projet de migration et de pouvoir réaliser la recette fonctionnelle de la migration entre mars et avril 2027, compte tenu de la disponibilité des équipes métier.

Les délais proposés par le titulaire dans son offre et validés par le Sénat deviennent contractuels.

ARTICLE 7. - Description des prestations attendues (prestations sur bons de commande)

En cas de nécessité, pour les prestations non incluses dans l'article 6 du présent CCTP, le Sénat sollicitera le prestataire, par l'émission de bons de commande, aux fins de réalisation de trois types de prestations présentées ci-dessous : des prestations d'assistance technique complémentaire post-migration, de formation, et d'ateliers de co-développement sur Oracle APEX.

La tarification de ces prestations sur bons de commande figure au bordereau des prix unitaires (BPU) du présent marché.

7.1. Prestation d'assistance technique complémentaire post-migration

À l'issue de la période de vérification du service régulier et à des fins d'accompagnement des équipes techniques, d'assistance à l'exploitation et d'optimisation des performances du dispositif migré, le titulaire pourra être sollicité par le Sénat pour l'intervention :

- d'un expert technique d'Oracle E-Business Suite, justifiant d'une expérience supérieure à cinq ans ;
- d'un expert technique d'Oracle Database, justifiant d'une expérience supérieure à cinq ans ;
- d'un expert technique d'Oracle Enterprise Command Center, justifiant d'une expérience supérieure à cinq ans.

7.2. Prestation de formation

Le titulaire propose les prestations de formation suivantes :

- deux sessions de formation d'une demi-journée pour l'administrateur système en charge des serveurs ;
- deux sessions de formation d'une demi-journée sur Entreprise Commande Center pour les utilisateurs clés (avec au maximum 5 utilisateurs par session).

7.3. Ateliers de co-développement sur Oracle APEX

Cette prestation a pour objet la réalisation de développements applicatifs au sein de la plateforme Oracle APEX selon un mode dit de « co-développement à quatre mains », associant de manière conjointe les ressources du titulaire et celles du Sénat.

La prestation couvre notamment la conception fonctionnelle détaillée des écrans et traitements APEX, le développement des composants applicatifs et la correction des anomalies identifiées en atelier, conjointement avec les équipes de la DSI du Sénat. Le titulaire assure un rôle d'expertise, de sécurisation technique et garantit le respect des bonnes pratiques APEX. Il est responsable de la qualité des développements réalisés.

La prestation est organisée sous la forme d'ateliers, en présentiel, incluant un ou plusieurs développeurs APEX expérimentés mis à disposition par le titulaire.

ARTICLE 8. - Compétences techniques attendues

Le titulaire devra justifier d'une expertise sur Oracle E-Business Suite 12.2 et Oracle Database 23 ou supérieure, prenant par exemple la forme d'une certification Oracle ou équivalent, et d'une expérience sur *a minima* plusieurs projets de migration similaires.

Le titulaire est déclaré attributaire du marché compte tenu de son organisation, de ses qualifications et références professionnelles et de celles de son personnel. S'il venait à perdre ces qualifications, le marché pourra être résilié sans indemnité.

ARTICLE 9. - Lieu d'exécution des prestations

Les prestations du présent marché sont réalisées principalement sur le site du Sénat à l'adresse suivante : 8 rue Garancière, 75006 Paris. Par dérogation, les parties prenantes peuvent convenir de modes de travail plus appropriés au bon déroulement de la prestation et plus économiques (audio-conférence, visio, etc.).

Le Sénat équipera les personnes présentes au Sénat d'un poste de travail Windows. Son utilisateur est tenu de respecter la charte d'utilisation des systèmes d'information du Sénat (cf. annexe n° 4). L'utilisation du poste de travail et des ressources mises à disposition des personnes par le Sénat sont exclusivement réservées à l'exécution de la prestation.

Une solution de travail à distance peut être mise à disposition par le Sénat si nécessaire, sous réserve que le lieu de télétravail demeure en France. Elle consiste en un accès Global Protect permettant la prise en main d'une VM Windows 11 mise à disposition par la DSI du Sénat. Le titulaire doit disposer d'une licence en cours de validité à la solution d'accès à distance TeamViewer.

ARTICLE 10. - Comitologie

10.1. Comité technique hebdomadaire

Un comité technique se réunit régulièrement, selon une fréquence définie conjointement entre les parties prenantes, et regroupe l'interlocuteur désigné par le titulaire et, pour le Sénat, le responsable administratif ainsi que les informaticiens en charge du projet à la DSI du Sénat.

Ce comité assure le suivi de l'avancement du projet.

Les réunions pourront se tenir à distance avec l'accord des deux parties.

10.2. Comité de pilotage

Le comité de pilotage est convoqué en tant que de besoin et réunit, a minima, pour le Sénat le responsable de domaine du pôle gestion, le responsable de la gestion et du suivi du marché, le responsable de domaine du pôle système de la DSI, les informaticiens en charge du suivi et de la mise en œuvre du projet et un représentant de la direction des affaires financières et sociales, et du côté du titulaire, le responsable du compte ainsi que l'interlocuteur unique désigné.

Ce comité a pour objet de contrôler le bon avancement du projet et d'effectuer les éventuels arbitrages requis.

En amont de chaque comité de pilotage, le titulaire adresse au Sénat les documents supports de la réunion. À l'issue de chaque comité il adresse au Sénat, pour validation, un projet de compte rendu de la réunion dans un délai de 5 jours ouvrés. À la demande du Sénat, il produit également tout type de document relatif au périmètre de cette réunion.

ARTICLE 11. - Principes de sécurité et données personnelles

Le prestataire doit mettre tout en œuvre pour assurer la sécurité des données, la sécurité du système applicatif et le refus d'accès non autorisés aux données du Sénat. Le transfert de données du Sénat à des personnes ou des sociétés non identifiées comme intervenants sur le présent marché ne peut en aucun cas être effectué sans un accord explicite du Sénat.

Aucune donnée applicative ne doit être exportée, copiée ou transférée en dehors de l'infrastructure informatique du Sénat, d'une quelconque manière.

Le titulaire s'engage à respecter la confidentialité et l'intégrité des données transmises, au même niveau de sécurité que l'environnement de production d'origine.

L'environnement contient un certain nombre de données à caractère personnel. Le titulaire n'est pas responsable du droit des personnes, comme l'information et la correction des données des personnes. Toutefois, si le titulaire est responsable d'une fuite, il devient responsable des dommages.

ARTICLE 12. - Réversibilité et transfert de compétences

Dans le contexte du présent marché, la réversibilité désigne la capacité pour la DSI du Sénat d'assurer en interne ou de confier à un tiers la gestion, la maintenance et l'évolution des solutions migrées (Oracle E-Business Suite et base de données Oracle) sans dépendance excessive vis-à-vis du titulaire, à l'issue du marché ou en cas de résiliation anticipée.

Le titulaire s'engage à :

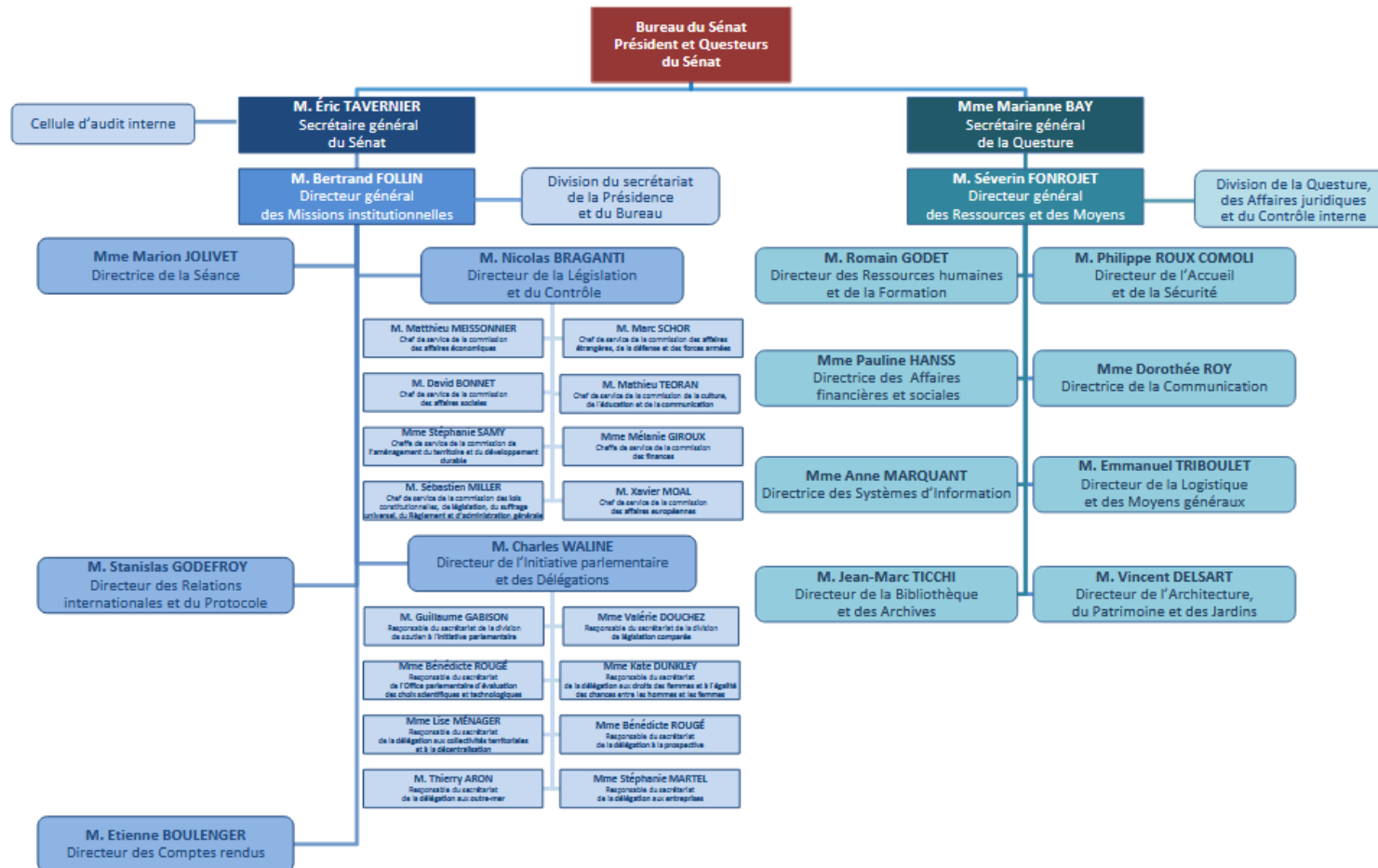
- documenter l'intégralité des processus de migration, de configuration, de maintenance et d'exploitation des environnements migrés, dans un document remis à la DSI du Sénat dans un format ouvert exploitable ;
- faciliter la transition en cas de rupture anticipée du contrat, en formant les équipes internes, assurant un support d'une durée minimale de deux mois pour accompagner la DSI du Sénat dans la reprise des activités et en transmettant l'ensemble des données et configurations dans un format ouvert exploitable.

En matière de transfert de compétences, la documentation exigée et les prestations de formation et d'assistance technique complémentaire prévues dans le cadre du présent marché doivent permettre aux équipes de la DSI du Sénat d'administrer les environnement Oracle installés en

autonomie, de maintenir et faire évoluer les solutions migrées et de résoudre les incidents courants.

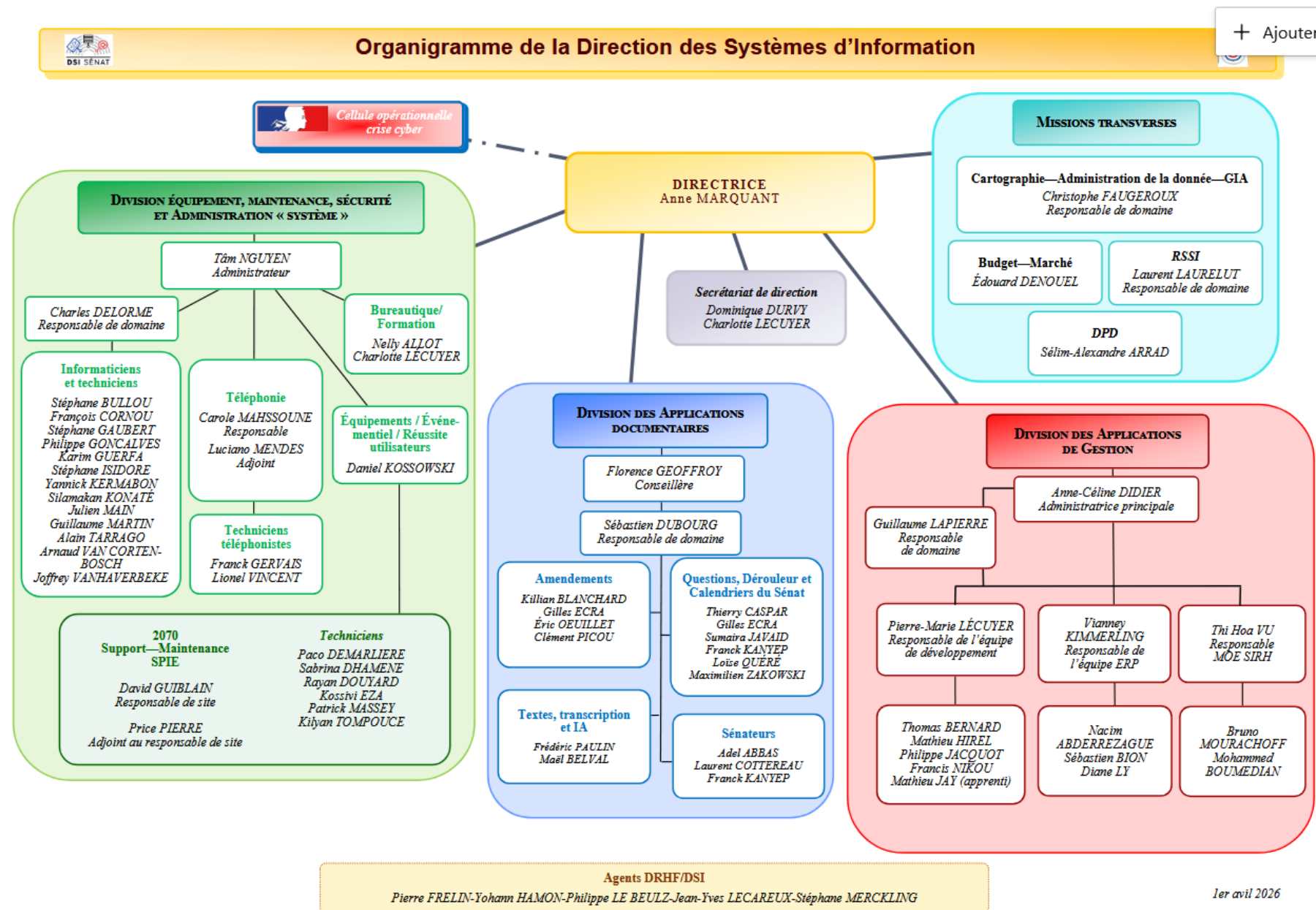
ANNEXES

Annexe 1 : Organigramme du Sénat

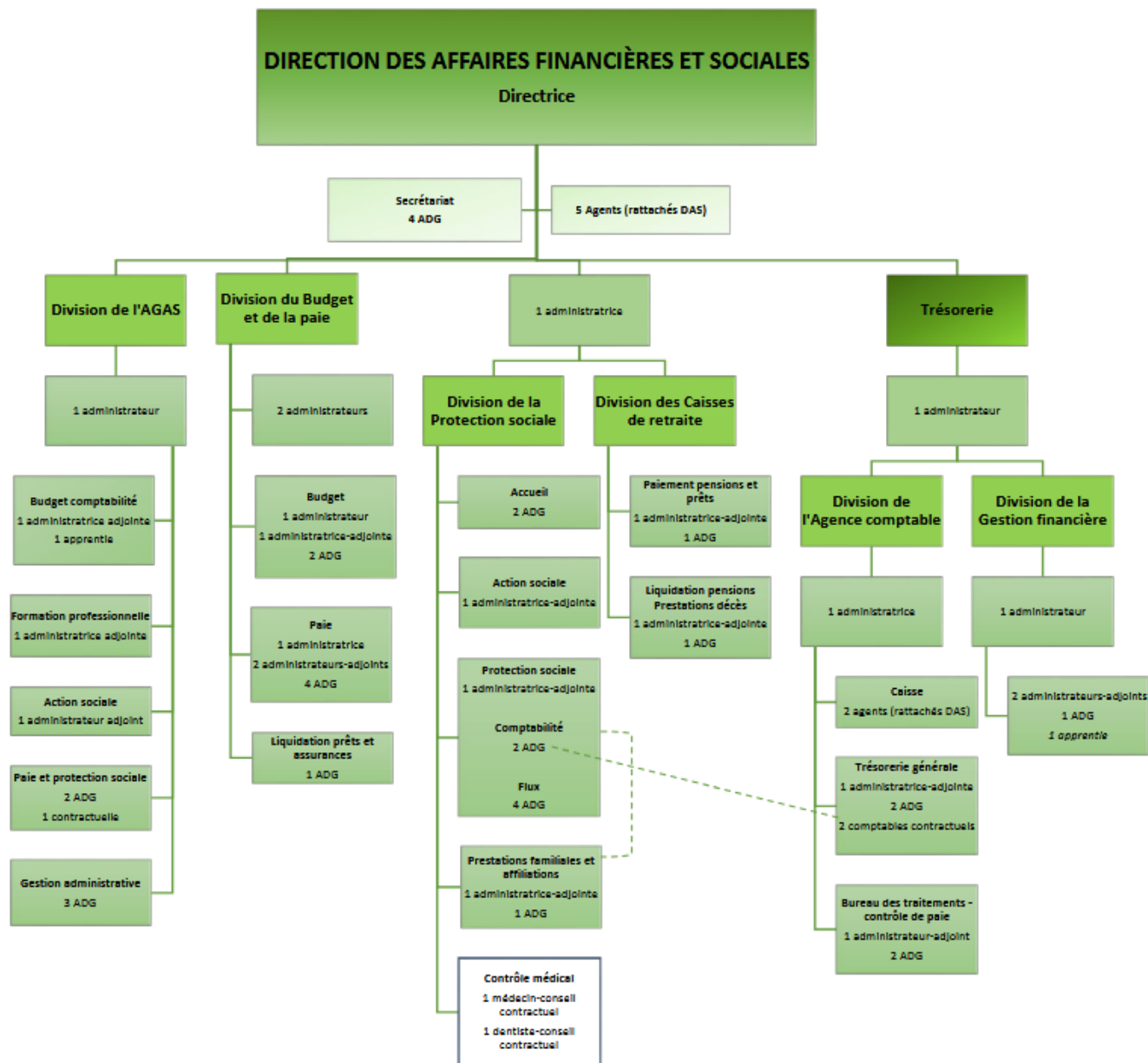


Organigramme administratif du Sénat au 1^{er} juin 2026

Annexe 2 : Organigramme de la Direction des systèmes d'information du Sénat



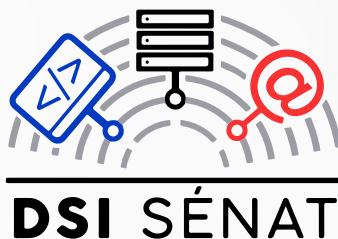
Annexe 3 : Organigramme de la Direction des affaires financières et sociales du Sénat



Annexe 4 : Charte d'utilisation des systèmes d'information du Sénat

2025

CHARTRE D'UTILISATION DES SYSTÈMES D'INFORMATION



SÉNAT



TABLE DES MATIÈRES

Préambule	2
I. Dispositions générales.....	2
Article 1 – Protection des composants des systèmes d'information et signalement des incidents.....	2
Article 2 - Accès aux réseaux informatiques et au réseau Internet.....	3
Article 3 – Confidentialité des accès.....	3
Article 4 – Nomadisme numérique	4
Article 5 - Respect des droits de propriété intellectuelle.....	4
Article 6 – Protection des données.....	4
Article 7 –Données à caractère personnel.....	5
Article 8 – Correspondance électronique.....	5
Article 9 – Sites collaboratifs et réseaux sociaux	6
Article 10 – Pratique éco-responsable	6
Article 11 – Contrôle de l'utilisation des équipements, logiciels et réseaux ..	6
II. Dispositions spécifiques.....	7
Article 12 – Préservation de l'intégrité des équipements.....	7
Article 13 – Protection des données et des documents professionnels	8
Article 14 – Responsabilité.....	8
Article 15 – Déplacements à l'étranger	8
Article 16 – Traitements de données à caractère personnel.....	9
Article 17 – Utilisation de systèmes d'intelligence artificielle	9
Article 18 – Utilisation privée des outils numériques du Sénat	9
Article 19 – Télétravail.....	10
Article 20 – Départ du Sénat.....	10
III. Dispositions finales	11

PRÉAMBULE

La présente charte décrit les règles de sécurité fondamentales et les bonnes pratiques à respecter lors de l'utilisation des systèmes d'information¹ (SI) du Sénat. Elle s'inscrit dans le cadre de sa Politique de Sécurité des Systèmes d'Information (PSSI).

Dans le respect des droits et libertés de chacun, ces règles et bonnes pratiques visent à limiter les risques techniques et juridiques qu'une mise en œuvre non maîtrisée ou inappropriée de ces technologies ferait courir tant à l'Institution qu'aux utilisateurs individuels. Elles garantissent ainsi la confiance dans les SI du Sénat.

La présente charte comporte, d'une part, les dispositions générales (articles 1 à 11) applicables à l'ensemble des utilisateurs ayant accès aux systèmes d'information du Sénat, notamment : les parlementaires et leurs collaborateurs, les personnels de l'administration et ceux des groupes politiques, les stagiaires et les prestataires du Sénat, et, d'autre part, les dispositions spécifiques (articles 12 à 20) applicables aux seules personnes dotées d'équipements numériques fournis par le Sénat.

I. DISPOSITIONS GÉNÉRALES

ARTICLE 1 – PROTECTION DES COMPOSANTS DES SYSTÈMES D'INFORMATION ET SIGNALEMENT DES INCIDENTS

Les SI du Sénat représentent un bien commun et partagé par tous leurs utilisateurs. Chacun doit éviter d'en perturber le bon fonctionnement en se conformant aux règles élémentaires de bon sens, en observant un devoir général de prudence et en appliquant les règles et principes énoncés dans la présente charte.

Malgré la mise en place par la direction des systèmes d'information (DSI) de dispositifs matériels et logiciels visant à assurer le bon fonctionnement et la sécurité des systèmes d'information du Sénat, chaque utilisateur joue un rôle essentiel dans leur protection.

Il ne doit pas tenter de contourner ces dispositifs de sécurité. S'il considère que certaines mesures ou règles ne sont pas légitimes, il doit le signaler au support informatique.

Chacun doit séparer strictement ses usages professionnels de ses usages personnels.

¹ Ensemble des infrastructures et services logiciels informatiques, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données.

Le branchement de périphériques de stockage externes sur des équipements connectés aux SI du Sénat doit faire l'objet de précautions particulières. Au moindre doute, l'utilisateur doit faire réaliser un test préalable du dispositif par le support informatique.

Toute présomption d'incident doit lui être signalée sans délai, par téléphone au 2070 ou via la création d'une requête sur le portail web (<https://support.senat.fr>).

ARTICLE 2 - ACCÈS AUX RÉSEAUX INFORMATIQUES ET AU RÉSEAU INTERNET

Les ressources offertes par les SI du Sénat doivent être utilisées uniquement par les personnes autorisées.

L'ouverture du droit d'accès aux réseaux informatiques disponibles dans l'enceinte du Sénat est subordonnée à une autorisation de la DSI.

Pour les visiteurs enregistrés auprès des accueils, seul le portail wifi est libre d'accès. Ses utilisateurs sont responsables aux termes de la loi de leurs usages de l'accès à Internet qui leur est offert.

La qualité de l'accès au réseau Internet depuis le Sénat repose en grande partie sur une utilisation raisonnable par chacun, en particulier, limitée à un strict besoin professionnel.

Chacun doit être attentif à la nature des sites qu'il consulte et des documents qu'il télécharge.

La navigation web sur Internet est protégée par une passerelle de sécurité qui effectue une analyse antivirus des flux de données à risque vers ou en provenance d'Internet et bloque les contenus malveillants. De plus les sites web ont tous été classés dans des catégories. Certaines de celles-ci, considérées comme non appropriées dans le cadre d'une utilisation professionnelle, entraînent l'impossibilité de consulter le site depuis le Sénat. En cas de détection d'une mauvaise classification d'un site ou en cas de besoin professionnel particulier, l'utilisateur est invité à le signaler au support informatique (cf. article 1).

ARTICLE 3 – CONFIDENTIALITÉ DES ACCÈS

Les identifiants et mots de passe permettant d'accéder aux différentes ressources du Sénat constituent des informations personnelles et confidentielles.

Les mots de passe doivent être robustes et changés à la moindre suspicion de compromission.

Des conseils pour la gestion des mots de passe sont disponibles sur le site intranet dans les pages de la DSI.

Pour les authentifications sur des sites extérieurs au Sénat, un mot de passe différent doit impérativement être choisi pour chaque site ou application. Le mot

de passe interne du Sénat ne doit en aucun cas être utilisé. L'usage d'une authentification multifactorielle doit être privilégié lorsqu'elle est disponible.

L'adresse de messagerie du Sénat ne doit pas être utilisée comme identifiant ou adresse de contact en dehors du cadre strictement professionnel.

Chaque utilisateur doit être attentif à toujours verrouiller son écran dès qu'il s'absente et à protéger ses moyens informatiques contre le vol.

| ARTICLE 4 – NOMADISME NUMÉRIQUE

Les équipements mobiles doivent faire l'objet d'une vigilance renforcée. Leur utilisation dans les lieux publics doit se faire avec la plus grande prudence. En particulier il convient de porter attention aux réseaux auxquels ils sont connectés et aux conditions de recharge de leurs batteries.

Les détails des règles à suivre pour gérer les équipements mobiles et lors des déplacements sont disponibles dans le guide du nomadisme numérique dans les pages de la DSI sur le site intranet.

En cas de déplacement à l'étranger, il est primordial de limiter au strict nécessaire les équipements et données emportées, voire de se doter d'équipements dédiés.

Au retour il est prudent de remplacer tous les mots de passe qui ont été utilisés lors du séjour.

En cas de perte ou de vol d'un équipement mobile, ou de compromission des informations d'authentification ou des données contenues dans les équipements, l'utilisateur doit impérativement alerter au plus vite le support informatique (cf. article 1).

| ARTICLE 5 - RESPECT DES DROITS DE PROPRIÉTÉ INTELLECTUELLE

Le téléchargement de fichiers ou de logiciels dont l'utilisateur ne détient pas les droits d'usage ou n'est pas en mesure de les acquérir est strictement interdit.

L'installation et l'utilisation de logiciels qui ne respectent pas les conditions générales d'utilisation de l'éditeur ou dont lesdites conditions mettent en cause l'intégrité des SI du Sénat est prohibée.

Il en va de même pour les services ou applications en ligne, en particulier si leurs conditions générales d'utilisation ne préservent pas les droits de propriété intellectuelle sur les informations de leurs utilisateurs.

| ARTICLE 6 – PROTECTION DES DONNÉES

Chaque utilisateur doit prendre toutes les dispositions pour s'assurer de la protection des informations et des documents numériques qui lui sont confiés et auxquels il a accès. Il doit appliquer les mesures de cybersécurité découlant de la classification de ces données ou, en l'absence de classification, évaluer leur

sensibilité et la traduire par des mesures appropriées pour leur manipulation au quotidien et pour leurs transferts vers d'autres environnements.

| ARTICLE 7 – DONNÉES À CARACTÈRE PERSONNEL

Le traitement dans les SI du Sénat de données à caractère personnel est soumis aux obligations du Règlement général sur la protection des données² (RGPD) et de la loi informatique et libertés³ (LIL).

Les données à caractère personnel sont celles se rapportant à une personne physique qui peut être identifiée directement ou indirectement, par croisement d'informations ou déduction.

Le Sénat a désigné un délégué à la protection des données (DPD) en charge de s'assurer de la conformité des pratiques du Sénat avec le RGPD et la LIL.

Chaque utilisateur dispose d'un ensemble de droits dont le droit d'accès et de rectification pour les données à caractère personnel le concernant, enregistrées dans les traitements du Sénat. Ces droits s'exercent auprès des responsables de traitements par l'intermédiaire du DPD (dpd@senat.fr).

| ARTICLE 8 – CORRESPONDANCE ÉLECTRONIQUE

Le Sénat met à disposition de tout utilisateur habituel de ses systèmes d'information une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

Il doit notamment avoir conscience que les messages qu'il envoie depuis cette adresse, se terminant par « senat.fr », engagent l'image de l'institution sénatoriale.

Il doit faire un usage raisonnable et conforme aux bonnes pratiques de cet outil de communication.

Les correspondances électroniques sont une des sources principales utilisées par les personnes malintentionnées pour perturber le fonctionnement des systèmes d'information ou tenter de les compromettre. En dépit des dispositifs de protection mis en œuvre, certains de ces messages sont malgré tout délivrés. L'utilisateur d'un système de communication électronique du Sénat doit par conséquent être vigilant quant aux messages qu'il reçoit et ne pas hésiter à contacter le support informatique au moindre doute sur leur légitimité (cf. article 1).

La mise en œuvre d'un système de renvoi automatique des messages vers une messagerie extérieure au Sénat, susceptible d'induire en erreur les expéditeurs et de mettre en danger les données contenues dans les messages est proscrite.

² Règlement général UE 2016/679 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

³ Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés

Des conseils plus détaillés sur l'utilisation de la messagerie électronique et sa sécurité sont disponibles dans les pages de la DSI sur le site intranet.

Ces bonnes pratiques de prudence dans les communications électroniques peuvent utilement s'appliquer aux messageries instantanées pour leurs aspects communs.

ARTICLE 9 – SITES COLLABORATIFS ET RÉSEAUX SOCIAUX

L'utilisateur de sites collaboratifs ou de sites ou applications des réseaux sociaux doit être conscient que mentionner son appartenance au Sénat, indiquer sa fonction ou utiliser son adresse de messagerie professionnelle dans une publication quelconque ou pour se connecter à un de ces sites est susceptible d'engager l'image de l'institution.

Il est par ailleurs averti que toute consultation d'un site depuis l'infrastructure du Sénat laisse une trace dans les journaux de ce site qui permet d'en identifier l'origine.

L'utilisation d'un espace de stockage partagé sur internet doit se faire en portant une attention particulière à la confidentialité et à l'intégrité des informations qui y sont copiées. Une copie locale de tous les documents qui y ont été transférés doit être impérativement conservée.

ARTICLE 10 – PRATIQUE ÉCO-RESPONSABLE

L'utilisateur des SI du Sénat doit adopter une pratique respectueuse de l'environnement.

Il lui est conseillé d'éteindre ses équipements numériques lorsqu'il ne les utilise plus, de limiter ses impressions et lorsqu'elles sont indispensables de privilégier l'impression recto-verso en noir et blanc sur des imprimantes partagées ou des copieurs.

La diminution de la fréquence de remplacement des équipements combinée à l'utilisation de matériels reconditionnés constituent les mesures les plus efficaces pour réduire son impact environnemental lié aux outils numériques.

Il est conseillé de se référer au document détaillant la stratégie environnementale du Sénat ainsi qu'aux recommandations figurant dans les pages de la DSI sur le site intranet pour orienter sa pratique en la matière.

ARTICLE 11 – CONTRÔLE DE L'UTILISATION DES ÉQUIPEMENTS, LOGICIELS ET RÉSEAUX

Dans le cadre de sa mission générale de gestion des SI du Sénat, la DSI a compétence pour analyser, limiter et contrôler l'utilisation des ressources matérielles, logicielles et des réseaux, afin d'en préserver la cybersécurité, d'en assurer le bon fonctionnement et de veiller au respect de la législation et des intérêts du Sénat.

Les personnels techniques de la DSI en charge de ces opérations ont l'obligation de préserver la confidentialité des informations qu'ils auraient été amenés à connaître, dans le respect du règlement intérieur et de la charte de déontologie qui lui est annexée.

Les journaux d'activité des différents composants (matériels et logiciels) des SI du Sénat enregistrent les informations techniques correspondant aux actions de leurs utilisateurs ou à leur propre fonctionnement. Un certain nombre de ces traces sont enregistrées de façon centralisée dans un système assurant la garantie de leur intégrité et de leur traçabilité pendant un (1) an. Elles sont automatiquement effacées à l'issue de ce délai.

II. DISPOSITIONS SPÉCIFIQUES

| ARTICLE 12 – PRÉSERVATION DE L'INTÉGRITÉ DES ÉQUIPEMENTS

L'utilisateur des moyens informatiques mis à disposition par le Sénat est responsable des matériels dont il est doté et ne doit pas les détourner pour un usage pour lequel ils n'auraient pas été prévus.

La configuration du matériel mis à disposition ne doit pas être modifiée.

Il est interdit de dissocier les composants des équipements fournis à titre professionnel dans le but de les intégrer dans des équipements personnels.

Dans la mesure du possible, l'utilisateur se doit de protéger les équipements qui lui ont été confiés contre le vol, la perte, les accidents ou l'utilisation non autorisée.

L'utilisateur d'un poste de travail ne peut procéder à l'installation de logiciels ou d'applications autres que ceux qui lui ont été fournis dans la configuration initiale de son équipement. Seule la DSI est habilitée à installer des logiciels supplémentaires ou à autoriser l'installation d'applications qui seraient nécessaires à ses besoins professionnels.

L'utilisateur d'un téléphone mobile professionnel peut installer les applications qui lui sont nécessaires depuis les magasins d'applications officiels, à l'exception de celles qui ont été explicitement interdites, dont la liste est disponible dans la page dédiée à la téléphonie mobile professionnelle des pages de la DSI sur le site intranet.

Toute souscription à un service en ligne dans le cadre d'une initiative personnelle ou d'une expérimentation doit faire l'objet d'une déclaration préalable à sa hiérarchie et à la DSI. En particulier il faut que les conditions générales d'utilisation (CGU) de ces services soient compatibles avec la présente charte et ne confèrent pas à l'éditeur de la solution des droits sur les documents et informations qui y sont traités.

Il est interdit à tout utilisateur d'effectuer des copies de logiciels dont les licences d'utilisation ont été attribuées au Sénat ou d'utiliser des applications ou abonnements à des services pris en charge par le Sénat, à des fins personnelles.

L'utilisateur doit régulièrement redémarrer son équipement et ne pas bloquer les opérations de mise à jour des applications ou l'installation des correctifs de sécurité.

ARTICLE 13 – PROTECTION DES DONNÉES ET DES DOCUMENTS PROFESSIONNELS

L'utilisateur doit impérativement sauvegarder, dans les espaces disques partagés des serveurs bureautiques, les documents professionnels stockés localement.

Il ne peut modifier ou supprimer que les données ou les fichiers qu'il a lui-même produits ou dont il assure la gestion. Il est responsable des créations, modifications ou suppressions de données ou de fichiers qu'il effectue.

L'utilisateur ne doit pas modifier des documents professionnels à partir d'équipements personnels.

Une analyse antivirus automatique des postes de travail est effectuée à intervalle régulier afin de détecter, a posteriori, des menaces passées initialement inaperçues.

Lors de la navigation web les flux chiffrés (hormis ceux à destination des sites bancaires) sont déchiffrés pour permettre leur analyse antivirus.

ARTICLE 14 – RESPONSABILITÉ

L'utilisateur doit se conformer à la circulaire des Secrétaires généraux relative à l'utilisation des réseaux sociaux professionnels, disponible sur le site intranet.

Les accès ouverts depuis un équipement attribué individuellement sont réputés être le fait de l'attributaire de l'ordinateur. Dans le cas d'un ordinateur affecté collectivement, les accès à Internet nécessitent l'identification de l'utilisateur et, dans ce cas, l'accès est considéré comme effectué par le détenteur du mot de passe associé à cet identifiant.

ARTICLE 15 – DÉPLACEMENTS À L'ÉTRANGER

L'utilisation des équipements habituels de l'utilisateur lors des déplacements professionnels à l'étranger est fortement déconseillée.

La DSI met à disposition, à la demande de l'utilisateur, des équipements dédiés nécessaires à l'accomplissement de ses missions. Certains équipements supplémentaires peuvent lui être confiés, sous sa responsabilité, pour être utilisés par les parlementaires qu'il accompagne.

D'autres dispositifs de sécurité peuvent lui être fournis à la demande (enveloppes de sécurité, bloqueurs de données USB, ...) et en tant que de besoin.

Les détails sont disponibles depuis la page de la DSI dédiée aux déplacements à l'étranger sur le site intranet.

ARTICLE 16 – TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Avant de constituer un traitement de données à caractère personnel, l'utilisateur doit obligatoirement en informer le DPD en vue d'un enregistrement dans le « registre des traitements de données à caractère personnel » du Sénat. Le DPD conseille et assiste le responsable de traitements ou les personnes à qui ce dernier a délégué certaines de ses responsabilités, afin d'assurer la sécurité juridique de ces traitements au regard du RGPD.

L'utilisateur, lorsqu'il est amené à manipuler des données à caractère personnel, doit veiller au respect :

- ❖ de l'information et de l'exercice des droits des personnes concernées ;
- ❖ de la communication au DPD des demandes d'exercices de droits qui lui seraient adressées ;
- ❖ des principes de minimisation et de proportionnalité des informations traitées ;
- ❖ de la confidentialité et de la sécurité des échanges.

ARTICLE 17 – UTILISATION DE SYSTÈMES D'INTELLIGENCE ARTIFICIELLE

L'utilisation dans le cadre professionnel de systèmes d'intelligence artificielle (IA), indépendants ou intégrés dans des applications, doit se faire dans le respect de la charte d'utilisation de l'IA, annexée au règlement intérieur du Sénat et disponible sur le site intranet.

ARTICLE 18 – UTILISATION PRIVÉE DES OUTILS NUMÉRIQUES DU SÉNAT

Les outils numériques mis à la disposition des utilisateurs sont destinés par principe à une utilisation professionnelle. En conséquence, tout fichier ou toute correspondance électronique qu'ils stockent sont présumés professionnels et peuvent être consultés, même en l'absence de l'utilisateur.

Il en va de même pour les données contenues dans tout équipement connecté à un poste de travail du Sénat.

Toutefois, un usage raisonnablement limité à titre privé des moyens bureautiques, de la messagerie électronique et de l'accès à Internet est toléré. Celui-ci ne doit affecter ni le bon fonctionnement et la sécurité des SI, ni l'image ou les intérêts du Sénat, pas plus qu'il ne doit créer une confusion avec l'activité professionnelle de l'utilisateur.

L'utilisation d'applications pouvant avoir un usage ambivalent doit être clairement séparée, en se servant d'identifiants différents pour chaque objet, l'adresse du Sénat étant réservée à un usage strictement professionnel.

Le stockage d'éléments personnels est autorisé uniquement sur le disque dur local et à condition que leur caractère privé soit explicite. Aussi l'utilisateur doit-il identifier clairement ses documents, placés dans un répertoire dédié, et ses messages personnels, en insérant une mention particulière dans leur sujet. Il est de sa responsabilité de veiller à ne pas stocker dans son espace personnel d'éléments ne respectant pas la législation en vigueur et en particulier les droits de propriété intellectuelle.

Les données stockées sur les disques durs locaux des postes de travail, à l'inverse de celles contenues dans les espaces disques partagés des serveurs bureautiques, ne sont pas couvertes par le dispositif de sauvegarde des données du Sénat. Il en est de même pour les messages stockés dans les « dossiers locaux » de la messagerie. Il appartient à chaque utilisateur d'en réaliser lui-même les sauvegardes.

Le raccordement d'équipements personnels au réseau informatique filaire du Sénat est interdit. Seule l'utilisation du réseau wifi est autorisée.

| ARTICLE 19 – TÉLÉTRAVAIL

Le télétravail est distinct du nomadisme numérique (cf. article 4).

Il fait obligatoirement l'objet d'une convention signée entre le télétravailleur et son directeur. Il s'effectue dans des lieux dont l'adresse est précisée à l'article 1 de ladite convention.

Tous les détails relatifs à la mise en œuvre du télétravail sont disponibles dans les pages de la direction des ressources humaines et de la formation (DRHF) sur le site intranet.

La localisation externe au Sénat des équipements impose au télétravailleur de prendre toutes précautions complémentaires pour en garantir autant que faire se peut leur sécurité et protéger les ressources auxquelles ils permettent d'accéder.

| ARTICLE 20 – DÉPART DU SÉNAT

L'utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles.

Lors de son départ, il doit restituer à la DSI l'ensemble des moyens numériques mis à sa disposition.

En cas de départ définitif, les comptes nominatifs et les données personnelles de l'utilisateur sont supprimés dans un délai maximum de 3 mois.

III. DISPOSITIONS FINALES

Portée à la connaissance de l'ensemble des utilisateurs lors de son entrée en vigueur, ou de sa révision, la présente charte est communiquée à toute nouvelle personne amenée à utiliser les équipements informatiques du Sénat ou susceptible de se connecter à l'un de ses réseaux. Elle est annexée au règlement intérieur et mise à disposition sur le site intranet du Sénat.

Elle n'a pas vocation à décrire de façon exhaustive toutes les situations possibles, mais à fixer des principes généraux. Il est de ce fait attendu des utilisateurs qu'ils agissent en respectant l'esprit de ces principes dans le cas où ils seraient confrontés à une situation qui n'y est pas mentionnée.

Pour toute demande de compléments d'information relatifs à cette charte, les utilisateurs sont invités à se rapprocher du responsable de la sécurité des systèmes d'information (RSSI – rssi@senat.fr).

Des modifications à la présente charte pourront être apportées en fonction de l'évolution du contexte réglementaire ou des changements de politique de sécurité des systèmes d'information du Sénat.

- Adoptée par le Bureau du Sénat le 5 février 2008 -
- Modifiée par l'arrêté de Bureau n° 2010-235 du 17 novembre 2010 -
- Modifiée par l'arrêté de Bureau n° 2015-146 du 25 juin 2015 -
- Modifiée par l'arrêté de Bureau n° 2025-325 du 30 octobre 2025 -