MINISTÈRE
DE LA TRANSFORMATION
ET DE LA FONCTION
PUBLIQUES

*Liberté*
*Égalité*
*Fraternité*

LES IRA

# Cahier des Clauses Techniques Générales TIC IRA

## Fourniture ou développement de services, applications et systèmes d'information

VERSION 1.0 DU 27/10/2023

Résumé

CCTG-TIC-IRA

Direction des programmes informatiques des IRA

Jean-luc.lagadec@ira-lyon.gouv.fr

TABLE DES MATIERES

**Chapitre. 1st.Généralités** ..... **3**
Article 1 Champ d'application ..... 3
**Chapitre. 2nd.Obligations spécifiques liées aux prestations d'herbergement** ..... **4**
Article 2 Hébergement ..... 4
**Chapitre. 3rd.Obligations spécifiques liées aux environnements des logiciels** ..... **12**
Article 3 Respect de l'état de L'art ..... 12
Article 4 Environnements logiciels ..... 12
Article 5 Sécurité de l'environnement ..... 13
Article 6 Fourniture du téléservice ..... 15
Article 7 Développement à façon du téléservice ..... 15
Article 8 Accessibilité, conformité, métrologie ..... 18
**Chapitre. 4th.Interoperabilite** ..... **20**
Article 9 Avec les navigateurs ..... 20
Article 10 Avec l'environnement des systèmes d'information des IRA ..... 20
Article 11 Avec l'environnement collaboratif des IRA ..... 21
Article 12 Avec l'environnement bureautique ..... 21
**Chapitre. 5th.Identification et authentification** ..... **23**
Article 13 Mécanismes d'identification et d'authentification ..... 23
Article 14 Délégation d'identification et d'authentification ..... 23
**Chapitre. 6th.Politique, gouvernance et organisation de la sécurite** ..... **25**
Article 15 Organisation de la sécurité ..... 25
Article 16 Gestion des biens ..... 26
Article 17 Sécurité physique ..... 27
Article 18 Sécurité des réseaux et de l'exploitation ..... 28
Article 19 Sécurité du poste de travail ..... 31
Article 20 Traitement des incidents ..... 31
Article 21 Disponibilité des données et des systèmes d'information ..... 31
Article 22 Continuité des services ..... 32
Article 23 Conformité, audit, inspection et contrôle ..... 32
Article 24 Obligations relatives aux astreintes ..... 32
Article 25 Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire ..... 33
Article 26 Protection des données personnelles ..... 34
**Chapitre. 7th. GLOSSAIRE** ..... **35**

| version | date | modification | rédacteur | valideur |
|---|---|---|---|---|
| **1.0** | 27/10/2023 | Version consolidée | JL LAGADEC | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Chapitre. 1er.
# GENERALITES

## Article 1
*Champ d'application*

Ce cahier de clauses n'est applicable qu'aux marchés qui s'y réfèrent.

Ces clauses visent des téléservices, applications dites « full web » à destination des usagers ou des agents, comprenant des pages d'information ou des saisies de données par formulaire et des transitions notables entre pages accessibles et mise en œuvre au travers d'un navigateur internet et les applications de type web-services par l'intermédiaire d'une API service web.

Leur contexte est celui de développements à façon. Pour des fournitures logicielles du marché, le respect des présents articles peut faire partie du processus de sélection d'un produit servant de base à un assemblage. Elles s'appliquent aux marchés publics qui ont un objet entrant dans le champ des techniques de l'information et de la communication (TIC). Il peut concerner notamment des marchés :

- de fourniture de logiciels commerciaux,
- d'études et de mise au point de logiciels spécifiquement conçus et produits pour répondre aux besoins particuliers,
- d'élaboration de systèmes d'information.

Ces articles constituent un standard de référence. Les développements et fournitures peuvent y déroger quand cela est stipulé dans le cahier des clauses techniques particulières (CCTP) du marché.

L'ordre des articles traduit une priorité des exigences en cas de conflit entre celles-ci.

- L'acte d'engagement et ses éventuelles annexes financières,
- Le cahier des clause administratives particulières (CCAP) ou tout autre document de clauses particulières (CCP),
- Le cahier des clauses techniques particulières (CCTP) ou tout autre document de clauses particulières (CCP),
- Le présent cahier des clause techniques générales – TIC IRA (CCTG – TIC IRA),
- Le cahier des clauses administratives générales – TIC (CCAG – TIC),
- L'offre technique du titulaire, dont le plan d'assurance sécurité (PAS),
- Les actes spéciaux de sous-traitance et éventuels actes modificatifs postérieurs à la notification du marché,
- La politique de sécurité des systèmes d'information (PSSI-E) de l'acheteur.

Chapitre. 2e.

# OBLIGATIONS SPECIFIQUES LIEES AUX PRESTATIONS D'HERBERGEMENT

## Article 2

*Hébergement*

### 2.1 Propositions d'hébergement

**2.1.1** Le téléservice doit pouvoir être hébergé suivant les principes de « cloud computing » définissant les types d'hébergement « en tant que service » : SaaS, PaaS ou IaaS.

**2.1.2** Le titulaire fournira, quand il est capacité de le proposer, deux propositions tarifaires :

- Une proposition pour un hébergement par le titulaire (SaaS ou PaaS avec sous-traitance de l'hébergement),
- Une proposition pour un hébergement par l'acheteur.

### 2.2 Hébergement par le titulaire (SAAS)

**2.2.1** En cas de fourniture du téléservice celui-ci pourra être hébergé par le titulaire (SaaS), suivant la sensibilité des données définies au CCP :

- Hébergement certifié ANSSI SecNumCloud pour les téléservices traitant des informations sensibles au titre de la doctrine cloud de l'Etat,
- Hébergement qualifié répondant aux exigences de la norme ISO/IEC 27001 relative au management de la sécurité des systèmes d'information, localisé sur le territoire national et non soumis aux droits d'extraterritorialité d'un pays tiers, pour les téléservices traitant d'information de moindre sensibilité,
- Hébergement répondant aux exigences relatives au management de la sécurité, définies au paragraphe 17.2 du présent CCTP-TIC et aux alinéas 2.2.4 à 2.2.22 du présent article, précisés dans le CCP, et localisé sur le territoire national, dans les autres cas.

La contractualisation des obligations vis-à-vis du responsable des traitements dans le cadre du RGPD est exigée.

Il peut être demandé dans le CCP que le titulaire réponde aux exigences des prestataires d'administration et de maintenance sécurisées (PAMS du 16/10/2022) : https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf)

**2.2.2** Dans le cas où le titulaire fait appel à une prestation de sous-traitance PaaS ou IaaS pour l'hébergement du téléservice, le sous-traitant est soumis aux mêmes exigences que le titulaire, particulièrement les exigences relatives au chapitre 6 « Politique, gouvernance et organisation de la sécurité » qui doivent être contractualisées.

La signature d'un contrat de confidentialité entre le titulaire et les sous-traitants est exigée.

Il peut être demandé dans le CCP que les sous-traitants répondent aux exigences des prestataires d'administration et de maintenances sécurisé (PAMS du 16/10/2022) : https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf.

**2.2.3** A défaut de conformité aux exigences définies à l'alinéa 2.2.1 du présent article, le téléservice sera hébergé sur les infrastructures cloud des IRA et devra répondre aux exigences des paragraphes 2.3, 18.3 et 24.3 « Hébergement par l'acheteur »

**2.2.4** Le candidat précise dans son offre les lieux géographiques dans lesquelles :

- Les données informatiques liées à la prestation seront hébergées ;
- Les services objets de la prestation seront localisés.

De même, le candidat précise dans son offre si ses infrastructures sont gérées ou simplement accessibles par une entité juridique appartenant à un pays disposant de lois autorisant ce pays à accéder aux données.

**2.2.5** Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité de ses infrastructures d'hébergement.

- phase de préparation ;
- phase de réalisation ;
- phase de vérification : préciser la fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du titulaire ou par une société tierce ;
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification).

**2.2.6** Une politique antivirale et anti-intrusion stricte devra être mise en place au niveau des serveurs dont le titulaire a la charge. La mise à jour des signatures devra être automatique et d'une fréquence élevée (30 minutes).

La politique antivirale appliquée sur le système d'information du titulaire devra être précisée (postes de travail des exploitants notamment).

Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se base les services de sa prestation (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

Un contrôle de non contamination des serveurs de production devra être effectué périodiquement et au minimum tous les mois. Le candidat précisera les modalités de mise en œuvre de ce contrôle.

**2.2.7** Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels et plateformes dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques) le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système de l'acheteur donneur d'ordres (serveurs, pare-feux, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERTA dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré-production.

Le titulaire devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à l'acheteur la version actualisée du document.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet de l'acheteur responsable de l'application hébergée.

En cas d'alerte émise par les équipes d'experts du titulaire, par l'administration ou le CERTA, l'acheteur sera notifié par téléphone et courrier électronique avant toute opération. La décision de l'action ne pourra être prise que par des personnels de l'acheteur désignés par écrit. En particulier, le responsable sécurité de l'acheteur sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, …) permettant à l'acheteur de suivre le traitement d'une alerte.

**2.2.8** Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé suivant une périodicité définie dans le CCP.

Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec.

La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration suivant une période définie au CCP, dont les rapports seront communiqués dans un délai d'un mois suivant les tests.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application de l'acheteur.

Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- confidentialité des flux lors des opérations de sauvegardes
- stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et de l'acheteur.

Dans le cadre de plans de sécurité gouvernementaux, l'acheteur pourra imposer une augmentation de la fréquence des sauvegardes.

**2.2.9** Le CCP précisera si besoin les conditions d'externalisation des sauvegardes vers l'infrastructure de stockage de l'acheteur.

**2.2.10** Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité du système d'information, conformément aux exigences définies dans la clause du CCP relative au niveau de service exigé.

Le candidat indiquera les mesures techniques, organisationnelles, procédurales qu'il s'engage à prendre pour assurer la continuité d'activité du système, ou en cas de sinistre la reprise d'activité, conformément aux exigences définies dans la clause sur la convention de service.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité.

**2.2.11** Tous les flux d'administration du titulaire vers l'hébergement doivent être chiffrés par des procédés (SSH, SSL, Ipsec, etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le candidat indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

**2.2.12** Au titre de la défense en profondeur, trois zones doivent être mises en place sur l'hébergement, chacune étant protégée par un dispositif de filtrage :

- une zone publique regroupant les machines qui hébergent les services ayant vocation à communiquer avec l'extérieur (Frontend applicatifs, passerelle d'API externe, Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS, etc.) ;
- une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés chez l'hébergeur.

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) sera fournie par le titulaire.

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés (filtrage sanitaire) notamment :

- attaque en déni de service (TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks, etc.) ;
- IP options (source routing, etc.).

Le candidat décrira dans sa réponse les différents mécanismes de protection prévus au niveau des équipements pour contrer les attaques classiques sur IP et les protocoles associés.

Les interfaces d'administration des machines ou des équipements du système ne doivent pas être accessibles depuis l'extérieur. Les services correspondants seront donc configurés pour ne pas accepter de connexions sur les interfaces publiques.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. Les autres services doivent être désactivés et si possible désinstallés.

**2.2.13** Lors des opérations d'infogérance les informations suivantes devront être enregistrées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ;
- création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

**2.2.14** Le titulaire précisera les mesures mises en œuvre pour assurer le recensement, la classification et le suivi des supports de données et équipements sensibles (boîtiers de chiffrement, pare-feux, etc.).

Le marquage des supports de stockage de données est obligatoire (disque dur, bandes de sauvegardes, etc.).

**2.2.15** Le titulaire s'engage à fournir une liste, mise à jour à chaque entrée/sortie de personnel, des personnels autorisés à intervenir sur l'hébergement ainsi que leur niveau d'habilitation (types d'accès et ressources concernées de l'acheteur).

Le candidat précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si des employés du candidat possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

Le candidat précisera dans son offre si d'autres clients peuvent accéder aux mêmes locaux que ceux utilisés pour le maître d'ouvrage et dans quelle mesure il sera possible de limiter ces accès à la demande éventuelle de ce dernier.

**2.2.16** Dans le cadre de plans de sécurité gouvernementaux, l'acheteur pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

**2.2.17** Le candidat indiquera dans sa réponse :

- les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations d'infogérance ;
- la fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité.

**2.2.18** Une solution de secours doit être mise en œuvre en cas de dysfonctionnement de l'alimentation électrique, de la climatisation ou des moyens de communication.

Le candidat décrira les moyens mis en œuvre afin d'assurer la continuité des services essentiels (énergie, climatisation, télécommunications) sur le site d'exploitation du système :

- situation et caractéristiques générales du site d'exploitation ;
- protection et redondance électriques (groupes électrogènes, onduleurs, protection contre les surtensions, etc.) ;
- contrats de service avec les fournisseurs d'accès, caractéristiques des liaisons de secours ;
- systèmes de climatisation ;
- moyens de supervision et remontées d'alarme ;
- les équipements utilisés par le système de l'acheteur, en particulier les composants redondants seront décrits (alimentations, disques, cartes contrôleurs, serveurs, équipements réseau, liens réseau) ;

Le candidat précisera les éventuels agréments gouvernementaux ou certificats de conformités qu'il détient.

**2.2.19** Le candidat décrira les moyens mis en œuvre en ce qui concerne :

- la prévention, la détection et le traitement des incendies ;
- la protection contre les dégâts des eaux ;
- la protection contre la foudre et les surtensions.

Il sera notamment indiqué dans la réponse si les bâtiments du site d'exploitation se situent ou non en zone inondable.

**2.2.20** Le site d'hébergement doit être surveillé 24h/24 et 7j/7.

Le titulaire doit mettre en œuvre un dispositif permettant de réserver l'accès aux locaux hébergeant l'ensemble des machines et postes de travail utilisés aux seules personnes autorisées par l'acheteur : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines. Il définira les conditions d'accès de l'acheteur au service (horaires d'ouverture, cas d'indisponibilité ponctuelle, etc.).

Le candidat doit détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux d'hébergement, notamment :

- moyens de surveillance, dispositifs anti-intrusion,
- contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.),
- protection physique des équipements (verrouillage des baies, etc.).

**2.2.21** Les intervenants des sociétés assurant la maintenance ou le support technique de solutions de l'acheteur doivent être accompagnés par une personne du prestataire habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l'imputabilité de ses actions.

Le candidat présentera les mesures techniques et organisationnelles mises en place pour empêcher les extractions massives d'information (par exemple : extraction d'une copie de la base de données à partir d'un poste dédié à l'administration).

Les supports de stockage de données (disques durs, bandes de sauvegardes, etc.) restent la propriété de l'acheteur. Ils ne peuvent être mis au rebut ou emportés par une société de maintenance, ni encore réutilisés à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

Ils doivent être conservés en lieu sûr par le titulaire, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée. L'effacement ou la destruction ont lieu en présence d'un représentant de l'acheteur.

**2.2.22** Le téléservice utilise un hébergement écoresponsable. Il bénéficie d'une efficacité énergétique au-dessus de la moyenne par une utilisation de la chaleur fatale ou a minima par un coefficient d'efficacité optimisé.

Pour éviter la pression sur l'artificialisation des sols, le réemploi de locaux d'hébergement est favorisé.

## 2.3 Hébergement par l'acheteur (IAAS)

**2.3.1** En cas de développement du téléservice, ou en cas de fourniture si le titulaire ne peut répondre aux exigences de l'alinéa 2.1.1, le téléservice sera hébergé sur l'infrastructure qualifiée SecNumCloud des IRA.

**2.3.2** Le titulaire fournira l'ensemble des prérequis système et documentation d'environnement, d'architecture et d'installation du téléservice.

Le titulaire conçoit ses livraisons en vue de l'automatisation complète des déploiements dans les environnements des bénéficiaires, y compris les configurations systèmes. A ce titre, il respecte les indications de l'hébergeur, ou, à défaut, les conventions d'usage pour les chemins de répertoires et fichiers, afin que les automates trouvent les composants.

**2.3.3** Le titulaire assurera l'infogérance et la tierce maintenance applicative du téléservice au travers d'un dispositif d'accès sécurisé (type bastion) mis à sa disposition et dont l'utilisation sera contractualisée.

Le périmètre et niveau de service d'infogérance seront défini dans le CCP.

Il peut être demandé dans le CCP que le titulaire réponde aux exigences des prestataires d'administration et de maintenances sécurisé (PAMS du 16/10/2022) : https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf

**2.3.4** Le titulaire s'engage à fournir une liste, mise à jour à chaque entrée / sortie de personnel, des personnels autorisés à intervenir sur le téléservice ainsi que leur niveau d'habilitation (types d'accès et ressources concernées de l'acheteur).

Le candidat précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

Le candidat indiquera dans sa réponse :

- les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations d'infogérance ;
- la fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité.

**2.3.5** La politique antivirale appliquée sur le système d'information du titulaire devra être précisée (postes de travail des exploitants notamment).

Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se base son service d'infogérance (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

Chapitre. 3e.

# OBLIGATIONS SPECIFIQUES LIEES AUX ENVIRONNEMENTS DES LOGICIELS

## Article 3

*Respect de l'état de L'art*

**3.1.1** Le titulaire conçoit, met en œuvre et exploite les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information et de développement. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière.

**3.1.2** Le titulaire est tenu d'assurer la sécurité des développements ou du produit fourni conformément à l'état de l'art dans chacune des technologies mises en œuvre.

- environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ; contrôle rigoureux des entrées utilisateurs ;
- sécurisation des accès aux fonctions d'administration ;
- installation du minimum de fonctions nécessaires lors de l'installation ;
- principe du moindre privilège ;
- utilisation de mots de passe dans le code interdite ;
- mise en œuvre d'une gestion efficace des erreurs.

La correction d'anomalies de sécurité détectées lors de la revue de code ou en production sont à la charge du titulaire.

## Article 4

*Environnements logiciels*

### 4.1 Généralités

**4.1.1** Quand cela est précisé dans le CCP, le téléservice sera multi-établissements . En fonction de l'utilisateur connecté ou de l'origine de l'appel au service, il pourra restreindre l'accès à un seul établissement et masquer la présence des autres.. Il permettra en particulier la mutualisation de données et de traitement pour ceux qui doivent être partagés entre les établissements.

**4.1.2** Quand cela est spécifié dans le CCP, le titulaire mettra à disposition un environnement de formation sur la base de la version du téléservice en production, alimenté avec des données dont les données personnelles auront été anonymisées, ou avec un jeu banalisé de données.

**4.1.3** Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il a la charge et doit les maintenir, selon les préconisations de l'ANSSI issues du guide « cartographie des systèmes d'information ». L'inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. La cartographie est livrée à la demande de l'acheteur.

**4.1.4** Le titulaire doit n'utiliser que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée du marché. A défaut, si la durée du marché dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

## Article 5

*Sécurité de l'environnement*

### 5.1 Securite

**5.1.1** Pour sécuriser le téléservice, les techniques suivantes sont mises en œuvre :

- https sur toutes les origines : les mécanismes cryptographiques TLS (HTTPS) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications,
- L'utilisation de la technologie HSTS est fortement recommandée quand le téléservice utilise les noms de domaine de l'acheteur,
- les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes,
- une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy)) est élaborée pour se protéger contre les injections de contenus actifs malicieux.

**5.1.2** Les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (TLS, STARTTLS, SMTPS, IMAPS, etc.) ;

La mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée :contrôle des noms de domaines associés au serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC).

**5.1.3** Dans le cas où le CCP précise que le nom qualifié de domaine du téléservice soit porté par les domaines de l'acheteur (ira.gouv.fr ou les-ira.fr) les certificats serveurs SSL seront certifiés RGS et fournis par l'acheteur.

Dans le cas où le nom qualifié de domaine est porté par le titulaire fournisseur du téléservice, les certificats SSL seront fournis par le titulaire.

**5.1.4** Une livraison peut être refusée si des composants ne sont pas à jours des correctifs de failles de sécurité publiés depuis un délai supérieur à 48 heures. L'acheteur définit les fréquences des livraisons en coordination avec les équipes d'exploitation, en fonction des différentes criticités des vulnérabilités concernées.

Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l'application du correctif.

**5.1.5** Pour les prestations, produits et services fournis dans le cadre du marché, le titulaire met à disposition un dispositif d'information dédié à la sécurité informatique (notamment flux RSS/ATOM, liste de diffusion par courriel ou autre).

Ce dispositif vise à tenir l'acheteur informé des événements et changements impactant la sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel), et des mesures correctives ou conservatoires à appliquer.

**5.1.6** Le titulaire est tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer l'acheteur des risques d'une opération envisagée, des incidents potentiels, et de la mise en œuvre éventuellement nécessaires d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le titulaire informera préalablement l'acheteur de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système au minium 48 heures ouvrées à l'avance.

**5.1.7** Le titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations :

- L'ensemble des systèmes quand le téléservice est hébergé par le titulaire,
- L'applicatif quand le téléservice est hébergé par l'acheteur.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

**5.1.8** Le titulaire devra collaborer pleinement en vue de l'homologation RGS du téléservice (cf RGS v2 : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/ ):

- Analyse des risques,
- Définition des objectifs de sécurité,
- Choix et mise en œuvre des mesures de sécurité adaptées,
- Homologation de sécurité du téléservice,
- Suivi opérationnel de la sécurité du téléservice.

Particulièrement, pour les téléservices qui l'exigent dans le CCP :

- Les règles relatives à la cryptographie,
- Les règles relatives à la protection des échanges électroniques (certificats d'authentification et de signature),
- Les règles relatives à l'horodatage électronique,
- Les règles relatives aux accusés d'enregistrement et aux accusés de réception,

**5.1.9** Dans le cadre de l'application de plans gouvernementaux, le Premier Ministre peut décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État.

Dans le cadre de ce marché, le titulaire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par l'acheteur. Ces mesures sont susceptibles d'évoluer. Les modifications seront régulièrement transmises par l'acheteur durant l'exécution du marché.

**5.1.10** Le titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité de l'information, des systèmes d'information et aux règles de l'acheteur.

Le titulaire veille notamment à ce que son personnel intervenant dans le cadre de des prestations respecte les dispositions concernant la sécurité du présent marché.

# Article 6

*Fourniture du téléservice*

## 6.1 Prestation de fourniture du téléservice

**6.1.1** Le titulaire est libre d'utiliser son propre environnement de développement, Framework ou progiciel à condition de respecter une architecture permettant l'isolation en couche n-tiers des objets présentation, métiers et données.

Le candidat présentera la documentation, l'intégration des recommandations de l'OWASP (Open Web Application Security Project), la revendication de conformité à l'ATAG-2 (accessibilité handicap) de son framework/progiciel.

**6.1.2** Le titulaire fournira et maintiendra à jour la liste (origine, version) de l'ensemble des composants tiers utilisés par le téléservice et non développés par ses soins.

Les composants tiers de type « extensions ou plugin » activant des dispositifs de traces (cookies) non maitrisés sont interdits.

**6.1.3** Le candidat fournira une cartographie complète de son environnement de développement, mise en production, réponse aux incidents techniques et de sécurité, implémentation en VA et VSR, diagramme des flux.

**6.1.4** L'ensemble des interfaces clientes IHM et web-services devront être accessibles par le protocole https.

Si cela n'est pas le cas, et si des interfaces IHM clientes sont conçues en mode 2-tiers client-serveur, les clients devront pourvoir être mis en œuvre sans installation sur les postes de travail et par des dispositifs d'accès distant (citrix, rdp,srvX, j2ee …) et uniquement à partir de réseaux isolés d'Internet (réseaux locaux, MPLS, SD-WAN, liens VPN, IpSec).

# Article 7

*Développement à façon du téléservice*

## 7.1 Prestation de développement du téléservice

**7.1.1** L'acheteur est propriétaire du code et des résultats de la prestation. Les droits de propriété, et exercice de ces droits, sont encadrés par l'article 46 du CCAG-TIC.

**7.1.2** Le téléservice devra être développé avec une répartition applicative de type n-tiers distincts.

L'architecture doit se diviser en couches logiques, permettant de mieux identifier les interactions mise en œuvre par le téléservice.

La structuration en couches d'une application permet de séparer la logique de présentation, de service et d'accès aux données.

Le couplage entre les couches applicatives doit être faible. A l'inverse le couplage entre les composants à l'intérieur d'une couche est fort.

Une architecture banalisée est plus facilement maintenable dans la mesure ou un nouvel intervenant est capable à partir de la description de l'architecture de comprendre le rôle de chaque composant développé et de s'insérer rapidement dans cette logique.

**7.1.3** Le titulaire utilisera des Frameworks de développement intégrant des fonctions de sécurité et disposant d'une communauté étendue et active, libres ou commerciaux, non propriétaires, en version LTS (long term support) orienté MVC (modèle-vue-contrôleur) ou MVP (modèle-vue-présentation), et répondant aux recommandations de sécurité de l'OWASP tant pour les composants backend que frontend.

**7.1.4** Le CCTG-TIC IRA n'impose pas de langage ni d'environnement de développement, mais il peut être précisé dans le CCP, particulièrement l'utilisation de framework ou de progiciels propriétaires au titulaire quand ceux-ci, après analyse, couvrent les exigences des alinéas ci-dessous.

Quel que soit l'outil de développement, les fonctionnalités de type modification, compilation ou déploiement doivent être accessibles sans disposer d'aucun environnement de développement intégré particulier.

**7.1.5** Il est avant tout conseillé de faire appel aux librairies open-source des organismes fiables pour assurer la mise en œuvre des couches techniques de l'application.

En cas d'utilisation de composants ou middleware commerciaux ou propriétaires, les éventuels coûts de licence et d'abonnement seront inclus dans le prix de la prestation.

Le titulaire fournira et maintiendra à jour la liste (sources et versions) de l'ensemble des composants tiers utilisés y compris les dépendances non natives du Framework (composer, npm, pip … ).

**7.1.6** Le titulaire mettra en œuvre autant que possible des modèles de conception réutilisables (design patterns) et la programmation orientée objet. Ces modèles de conception fournissent un support utile pour la mise en œuvre d'application flexible, modulaire.

**7.1.7** Les objets métiers ne doivent pas avoir connaissance des mécanismes de stockage qui leur sont attachés. Ces mécanismes sont accessibles au sein de la couche d'accès aux données.

Si possible la couche de persistance est fournie par le modèle de conception appelé DAO. Celle-ci fournit ses services par le biais d'un objet façade afin de les isoler.

Dans le cas contraire une technologie de mapping objet (ORM) sera obligatoirement utilisée afin de supprimer les adhérences aux technologies de stockage.

**7.1.8** Les interfaces de type contrôleurs exposées sur Internet doivent être isolées et distinctes pour les contrôleurs de type IHM et de type web-service.

Il est interdit de court-circuiter le modèle en couche lors de la mise en œuvre d'AJAX sur les frontend. Les services doivent être implémentés dans la couche de présentation en respectant le modèle n-tiers.

**7.1.9** Le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.

**7.1.10** Les livrables seront hébergés sur des environnements d'exploitation virtualisés pour des hôtes Linux Ubuntu ou Debian ou Windows Server 2019 en version LTS, les environnements serveurs applicatifs/web (Apache, Nginx, IIS, TomCat), de base de données (MariaDB, PostgreSQL, SQL Server) qui doivent être isolées des frontend ; en excluant tout dispositif tiers adhérent à une technologie ou licence particulière.

Les environnements d'exploitation open-source seront privilégiés.

**7.1.11** Les livrables conteneurisées de type Docker sont acceptés à condition qu'ils puissent s'exécuter dans un environnement sans orchestrateur (CaaS), et sans adhérence au système d'exploitation hôte sous-jacent.

Les montées de version incluent les migrations automatisées de données (entités ORM, schéma SQL, stockages de tables, etc.)

**7.1.12** Le code est partitionné et variabilisé selon les indications définies avec l'acheteur, par exemple entre la source du code principal et les sources des configurations des différents environnements.

Le titulaire suit la politique de gestion des versions indiquée par l'acheteur. A défaut, il utilise les conventions de gestion sémantique de version https://semver.org/lang/fr.

En période de développement, le titulaire réalise une livraison régulière, au rythme défini au démarrage du projet et fixé par la période des itérations, dans un état stable et susceptible d'être déployée.

La livraison de sources comprend la description exhaustive des dépendances et des chaînes d'outils permettant à l'acheteur de reproduire les livrables à partir d'outils dont il dispose.

Le titulaire alerte si les technologies qu'il utilise ne permettent pas des constructions reproductibles https://reproducible-builds.org/.

Le format de livraison est choisi par l'acheteur dans le CCP. A défaut d'indication, le titulaire fournit des paquets au format natif des plateformes cibles utilisées pour les déploiements : .msix pour Windows, .deb pour Debian, .oci pour Docker, etc. Dans ce cas, les pratiques des plateformes s'appliquent (nommage, répertoire par défaut, etc.).

**7.1.13** Le titulaire dispose d'un environnement de tests permettant de reproduire le comportement du téléservice et de réaliser les tests unitaires avant mise en production des évolutions (VA technique et fonctionnelle). Lors de la conduite de tests de validation ou du déploiement, le titulaire doit :

- utiliser des données de tests anonymisées ;

- ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de test ;
- remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible
- ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente

**7.1.14** La documentation technique associée à l'application doit être livrée sous deux formes :

1. Texte en respectant les règles d'écriture standard de la documentation technique relative au langage
2. Une documentation UML 2.0 avec format d'échange XMI.

Le diagramme de classe doit être présent dans la documentation UML.

Le diagramme de séquence est conseillé afin de mieux comprendre les interactions dans l'application.

**7.1.15** Le framework devra disposer de composants permettant la réalisation de tests unitaires en VA, fournissant un support à l'évaluation et l'exécution des tests.

Le test unitaire vérifie qu'un package ne comporte pas d'erreur de conception ou de programmation.

La recette comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité.

Les tests unitaires doivent être prévus au moment du développement pour les composants importants de l'application. Ceux-ci doivent permettre aussi la vérification des composants techniques et ainsi de contrôler la connectivité.

Le titulaire inclut dans ses livraisons, des tests automatisés et documentés qui permettent de franchir les étapes de la chaîne d'intégration (construction, déploiement…) sans régression.

# Article 8

*Accessibilité, conformité, métrologie*

## 8.1 Accessibilité et ergonomie

**8.1.1** Le téléservice devra respecter l'application des recommandations du RGAA (Référentiel Général d'Amélioration de l'Accessibilité - https://accessibilite.numerique.gouv.fr ).

En particulier, le téléservice soigne ses techniques et pratiques d'assistance aux diverses formes de handicaps, et dépasse un premier palier de 75 % des indicateurs.

**8.1.2** Le titulaire fournira les résultats d'audit RGAA, dans la version courante du règlement à la date de la consultation, permettant de définir en détail le niveau d'accessibilité du téléservice.

**8.1.3** Le téléservice devra suivre les recommandations de « La marque de l'Etat » publié par le Service d'Information du Gouvernement (SIG -

https://www.gouvernement.fr/marque-Etat), particulièrement pour les téléservices exposés sur Internet avec le nom de domaine ira.gouv.fr.

Le téléservice soigne la présentation des pages d'erreurs (codes 4xx, 5xx) et les intègre dans la charte graphique. En particulier, la page de ressource inexistante (404) propose des destinations alternatives. Ces pages n'exposent pas d'informations techniques sur les systèmes sous-jacents (nom et version du service http par exemple).

En cas de fourniture du téléservice, a minima les pages exposées sans authentification (la page d'accueil publique, la page d'identification et les pages d'erreur, contacts, mention légales …) devront obligatoirement respecter la charte graphique.

Le titulaire privilégiera l'utilisation des composants du système de design de l'Etat (https://www.systeme-de-design.gouv.fr/) qui facilite le respect de la charte graphique et du référentiel général d'accessibilité.

## 8.2 Métrologie

**8.2.1** Le téléservice est équipé pour le suivi globalisé de sa fréquentation. Cela n'implique pas un traçage individualisé des visites.

**8.2.2** Le téléservice assure la maîtrise de l'ensemble des données de métrologie en conformité avec le règlement général sur la protection des données (RGPD).

**8.2.3** Le titulaire fournit les points d'intégration avec les pratiques de métrologie, journalisation et supervision de l'acheteur précisées dans le CCP.

A défaut d'indication, le titulaire suit les préceptes de « 12 facteurs » https://12factor.net/fr/.

## 8.3 Publications standardisées

**8.3.1** Le téléservice répond aux chemins suivants :

- /contacts ou équivalent pour offrir des options de contacts par téléphone, par courrier ou rendez-vous ;
- /mention-legales ou équivalent pour remplir les obligations d'information sur le responsable de publication, l'hébergeur, le niveau d'accessibilité et les objectifs de développement durable ;
- /.well-known/security.txt pour permettre le signalement en urgence de faille de sécurité.
- Mention légale RGPD.

## 8.4 Dossiers de conformité

**8.4.1** Le titulaire fournisseur du téléservice contribue à la préparation de :

- la fiche Registre et l'analyse d'impact de la protection des données pour les évaluations CNIL/RGPD ;
- l'évaluation d'accessibilité pour la conformité au RGAA ;
- l'homologation de sécurité pour le RGS ;
- l'évaluation d'écoconception vis-à-vis du RGESN.

Chapitre. 4e.
# INTEROPERABILITE

## Article 9
*Avec les navigateurs*

**9.1.1** Le titulaire a la responsabilité de maintenir le téléservice compatible avec les 5 premiers navigateurs web en usage en France, suivant à date du marché, les statistiques publiques diffusées sur GlobalStats https://gs.statcounter.com/browser-market-share/all/france/.

**9.1.2** Le téléservice est utilisable sur un terminal avec un écran de 12 cm en diagonale. Le design s'adapte aux écrans des ordinateurs de bureau, jusqu'à 72 cm.

Le téléservice reste compatible avec un terminal âgé de 5 ans mis à jour pour son navigateur, pour ne pas inciter au renouvellement de matériel.

**9.1.3** Le téléservice conserve des performances acceptables avec la bande passante et la latence de réseaux mobiles définis comme référencé par l'ARCEP dans son rapport annuel à la date du marché. Il limite le poids des pages du fait des abonnements mobiles à trafic mensuel limité

**9.1.4** Le téléservice utilise exclusivement les balises, attributs, composants et comportements HTML 5 et CSS conforme au W3C. Le balisage HTML 5 et CSS assure la meilleure compatibilité avec les navigateurs pour personnes handicapés, traducteurs automatiques et autres aides à la navigation.

Javascript est utilisé comme amélioration progressive et non comme un prérequis. Il est obligatoire d'utiliser des langages de script conformes à la norme ISO 16262 (langage ECMA script).

La norme d'encodage ISO 10646 et la recommandation UNICODE (utf-8) seront utilisées.

**9.1.5** Les ressources web sont accessibles par des URL stables pour conserver des références par lien.

## Article 10
*Avec l'environnement des systèmes d'information des IRA*

**10.1.1** Quand le téléservice doit proposer des services d'interopérabilités, d'échange de données et de délégation de fonctions inter-applicative sous forme d'API web-service, ceux-ci devront être conforme au Référentiel Général d'Interopérabilité (RGI) v2 publié par la Direction Interministérielle du Numérique (DINUM)

https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf

Particulièrement le profil d'interopérabilité P1 (Fondation Etat Plateforme) qui constitue le socle de base d'interopérabilité et défini le style d'architecture RESTful pour les API et le format JSON, encodage utf-8, pour la structuration des informations.

**10.1.2** Les échanges inter-applicatifs se feront au travers d'un dispositif passerelle API : API Manager ou Entreprise Service Bus hébergé sur l'infrastructure cloud des IRA.

**10.1.3** Les mécanismes d'accès authentifiés inter-applicatifs A2A doivent se faire au travers de connexions chiffrées et par des protocoles d'authentifications référencés OpenId Connect / Oauth 2.0.

**10.1.4** Exceptionnellement, et particulièrement si les échanges inter-applicatifs sont de type transactionnel long, le profil P1 pourra être étendu au profil P2 de type web service SOAP/XML/utf-8.

**10.1.5** Le téléservice devra être en mesure d'accepter l'implémentions de nouvelles interfaces API bidirectionnelles quand elles ne sont pas natives afin d'assurer l'interopérabilité avec le SI des IRA et ses évolutions.

Les besoins d'interfaces spécifiques seront exprimés dans les CCP.

## Article 11

*Avec l'environnement collaboratif des IRA*

**11.1.1** Dans tous les cas, le téléservice devra être en capacité de mette en œuvre des envois de courriels a minima par le protocole SMTPS authentifié à partir d'une ou plusieurs adresses mail définies par l'acheteur.

**11.1.2** Le téléservice devra être en capacité de s'interfacer avec l'environnement collaboratif de messagerie de d'agendas des IRA quand cela est spécifié dans le CCP :

- Délégation d'envoi de courriels en tant qu'utilisateur connecté,
- Délégation de mise à jour d'agendas,
- Capacité de réception de mails par le protocole IMAPS.

## Article 12

*Avec l'environnement bureautique*

**12.1.1** Quand le téléservice génère ou permet de manipuler des documents de type bureautique modifiables, ceux-ci devront être générés dans des formats référencés au Référentiel Général d'Interopérabilité (RGI) v2.

- Obligatoirement : le format ODF Open Document Format,
- Quand précisé dans le CCP : OOXML Office Open XML strict (docx, xlsx).

**12.1.2** Le format des documents non modifiables est le format PDF (Portable Document Format).

**12.1.3** Quand le téléservice génère des informations en capacités de s'interfacer avec les fonctions de publipostage des suites bureautiques, ces fonctions devront être compatibles avec :

- La suite LibreOffice,
- Quand précisé dans le CCP, la suite Microsoft Office.

Chapitre. 5e.
# IDENTIFICATION ET AUTHENTIFICATION

## Article 13
*Mécanismes d'identification et d'authentification*

**13.1.1** Le téléservice maintiendra des capacités d'authentification propre en cas de défaillance du fournisseur d'identité, particulièrement pour les comptes d'accès permettant l'administration du téléservice au travers d'une interface ou route d'accès dissociée.

**13.1.2** En complément des possibilités offertes via les API, le téléservice doit proposer des procédures d'importation de comptes utilisateurs par fichiers dans un format texte et encodage non propriétaire. Par exemple CSV, XML, JSON, YAML.

**13.1.3** Le service local d'identification du téléservice doit permettre l'initialisation et la réinitialisation du mot de passe par l'utilisateur par une procédure sécurisée de type échange de mail et activation de compte.

Les caractéristiques des mots de passe doivent répondre aux exigences de la PSSI-E.

## Article 14
*Délégation d'identification et d'authentification*

**14.1.1** Le téléservice devra être en mesure de s'interfacer et de déléguer l'authentification des utilisateurs à un ou plusieurs services tiers fournisseur d'identités utilisant le standard Open Id Connect avec l'algorithme « authorization code flow » basé sur le protocole Oauth 2.0 et SAML v2.

**14.1.2** Le téléservice doit être mesure de conserver, d'exploiter et de renouveler les informations d'identification de session déclenchées par la mise en œuvre du processus du fournisseur d'identité à partir d'une autre application sur la même session de navigation sans demander une nouvelle identification quand le fournisseur d'identité le permet (SSO).

**14.1.3** Dans le cas où il est demandé dans le CCP de pouvoir déléguer l'authentification à la fédération d'identité de l'Etat « AgentConnect », le téléservice devra répondre aux exigences d'homologation RGS et aux prérequis définis dans les conditions générales d'utilisation du service « AgentConnect » https://github.com/france-connect/Documentation-AgentConnect/tree/main/doc_fs/cgu_fca.

**14.1.4** Les processus d'habilitation par profil, sur les traitements et données du téléservice, restent à la charge de ce dernier.

Dans le cas où les processus d'identification et d'authentification permettent la création d'un nouveau compte utilisateur sur le téléservice une politique d'habilitation « Zero Trust » sera appliquée sur les nouveaux comptes.

**14.1.5** Quand précisé dans le CCP, le téléservice sera multi-établissements. En fonction du profil de l'utilisateur connecté ou de la route d'appel au service, il pourra restreindre l'accès à un seul établissement et masquer la présence des autres, tout en conservant les capacités de mutualisation de données et de traitement pour ceux qui doivent être partagés entre les établissements.

**14.1.6** Un système de trace des accès et horodatage des traitements sensibles doit être disponible aux administrateurs du téléservice.

Chapitre. 6e.

# POLITIQUE, GOUVERNANCE ET ORGANISATION DE LA SECURITE

## Article 15

*Organisation de la sécurité*

**15.1.1** Le titulaire applique et fait appliquer aux sous-traitants la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants:

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

**15.1.2** Le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.

Il communique à l'acheteur son plan d'assurances sécurité (PAS).

**15.1.3** Le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment :

- L'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;
- Ce correspondant est joignable aux horaires définis dans le CCP et à défaut tous les jours ouvrables de 09h00 à 18h00. Tout remplacement de ce correspondant doit être notifié à l'acheteur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

**15.1.4** Le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

**15.1.5** Sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés.

Ce plan précise au minimum :

- les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- la composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

## Article 16

*Gestion des biens*

**16.1.1** Le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire.

Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

**16.1.2** Le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

**16.1.3** Le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

**16.1.4** Le titulaire garantit que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'acheteur.

**16.1.5** Toute transmission de fichiers sur un support physique, par courrier externe ou par porteur, donne lieu à un accusé de réception.

Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'acheteur.

De plus, l'ensemble des opérations de transfert de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- l'émetteur et le destinataire ;
- le détail des opérations de transferts et notamment le nombre, la date.

Sur simple demande, ce registre est mis à la disposition de l'acheteur adjudicateur par le titulaire.

**16.1.6** Le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.

**16.1.7** Le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'acheteur, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

**16.1.8** Le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation

## Article 17

*Sécurité physique*

**17.1.1** Les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

**17.1.2** Le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

### 17.2 Hébergement du téléservice par le titulaire

**17.2.1** En cas de changement de localisation des données ou services, le titulaire en informe préalablement l'acheteur.

**17.2.2** A la première demande de l'acheteur, le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

**17.2.3** Le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le titulaire dispose d'une procédure de gestion des accès physiques à ses locaux techniques. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'acheteur et les équipements de sureté.

**17.2.4** Les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.
- Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

**17.2.5** En cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'acheteur (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'acheteur, etc.).

**17.2.6** Les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de l'acheteur n'a pas de murs adjacents à d'autres bureaux.

Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'acheteur de celles des autres clients au sein des salles informatiques.

**17.2.7** La salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée.

**17.2.8** Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

## Article 18

*Sécurité des réseaux et de l'exploitation*

### 18.1 Dans tous les cas

**18.1.1** Le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

**18.1.2** Le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautiques du titulaire.

**18.1.3** L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par la PSSI de l'acheteur. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'acheteur.

**18.1.4** Le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation.

**18.1.5** Le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'acheteur) dispose d'un compte individuel qui peut être :

- soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
- soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

**18.1.6** Le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut de livraison devront être systématiquement modifiés.

**18.1.7** Dans le cadre de la cartographie du système d'information prévue aux alinéas 4.1.3 et 6.1.3 du présent CCTG-TIC IRA, le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

**18.1.8** Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés.

Il fournit cette liste à l'acheteur sur demande.

Le titulaire effectue et formalise une revue périodique* des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

*une revue « d'emploi » (a minima trimestrielle), une revue de « besoin » (a minima annuelle).

**18.1.9** Le titulaire s'assure que tous les comptes des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

**18.1.10** Les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification. Exemple : blocage pendant 30 minutes de la session d'un poste de travail après 3 tentatives de connexion échouées.

**18.1.11** Le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves.

Le titulaire collecte et stocke à minima les informations suivantes :

- connexion et déconnexion aux équipements et applications ;
- consultations d'informations relatives à la vie privée ;

- informations d'usage de l'Internet (accès aux sites Web) ;
- accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
- informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

**18.1.12** Le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

**18.1.13** Le titulaire respecte la politique de définition des mots de passe de l'acheteur (https://www.ssi.gouv.fr/guide/mot-de-passe) sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

**18.1.14** Le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'acheteur dans le cadre de la prestation.

## 18.2 Hébergement du téléservice par le titulaire

**18.2.1** La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'acheteur.

**18.2.2** Le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de sécurité de l'ensemble de ses équipements pour les services fournis à l'acheteur.

**18.2.3** Le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés dans le CCP de l'acheteur dans le cadre de la prestation.

Des tests périodiques (de période définie sans le CCP) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués

**18.2.4** Le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

## 18.3 Hébergement du téléservice par l'acheteur

**18.3.1** Le titulaire accèdera aux ressources à travers un dispositif de contrôle des accès de type bastion, tant pour les sessions d'administration et d'infogérance que de déploiement de données et fichiers sources.

## Article 19

*Sécurité du poste de travail*

**19.1.1** Le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivol de façon systématique.

**19.1.2** Une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

## Article 20

*Traitement des incidents*

**20.1.1** Le service de supervision du titulaire met en place un système de remontée d'alerte à l'acheteur, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'acheteur (documentations techniques en particulier).

**20.1.2** Le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

**20.1.3** Le titulaire contacte les interlocuteurs sécurité de l'acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'acheteur. De plus :

- si cet incident a lieu sur le SI de l'acheteur, le titulaire participera à la demande de l'acheteur au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'acheteur ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'acheteur (traitement des causes profondes).

**20.1.4** Le titulaire capitalise les procédures de résolution des problèmes récurrents dans une base de connaissance dédiée qu'il fournit à l'acheteur sur demande.

## Article 21

*Disponibilité des données et des systèmes d'information*

**21.1.1** Durant le marché, le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information au niveau précisé dans le CCP.

En cas de non-respect de ces engagements, l'acheteur applique les pénalités visées dans le CCP, à défaut celles de l'article 14 du CCAG-TIC.

## Article 22

*Continuité des services*

### 22.1 Hébergement du téléservice par le titulaire

**22.1.1** Le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat dans les délais maximums définis au CCP. Il fournit, à la demande de l'acheteur, la preuve de l'existence d'un plan de continuité d'activité régulièrement testé pour l'ensemble des services fournis à l'acheteur.

L'acheteur se réserve le droit de demander les résultats des exercices de continuité d'activité réalisés par le titulaire.

**22.1.2** Le titulaire prend toutes les dispositions nécessaires (matériel en spare, contrats de service), en relation avec l'acheteur, pour remplacer rapidement et sur les différents sites de l'acheteur tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).

**22.1.3** En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'acheteur selon la procédure d'alerte qu'il a définie dans le CCP (directive de gestion des alertes, incidents et situations de crise).

## Article 23

*Conformité, audit, inspection et contrôle*

**23.1.1** Le titulaire effectue des autocontrôles de conformité aux exigences du CCP pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

**23.1.2** En cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation devra être formalisé par le titulaire 15 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

## Article 24

*Obligations relatives aux astreintes*

### 24.1 Dans tous les cas

**24.1.1** Le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte.

**24.1.2** Le titulaire rend obligatoire l'utilisation de l'authentification forte (ex. badge, token) au poste de travail utilisé en astreinte.

**24.1.3** Le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires ouvrés), et aux ressources nécessaires en astreinte uniquement.

### 24.2 Hébergement du téléservice par le titulaire

**24.2.1** Quand le téléservice est hébergé par le titulaire, le titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements. Les cas de force majeure doivent également être couverts.

### 24.3 Hébergement du téléservice par l'acheteur

**24.3.1** Quand le téléservice est hébergé par l'acheteur, le titulaire a l'obligation d'utiliser les services d'accès distants mis à disposition par l'acheteur.

En cas d'impossibilité d'utiliser le service d'accès distant de l'acheteur, le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN, IPSec) pour la connexion à distance en astreinte aux réseaux utilisés dans le cadre de la prestation (que ce soient ceux du titulaire, ceux de l'acheteur ou les deux éventuellement). Le personnel du titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès aux SI à distance (connexion authentifiée non permanente).

## Article 25

*Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire*

**25.1.1** Au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

**25.1.2** Le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur et figurant au présent CCTG-TIC IRA (Bastion SSL pour l'infogérance, API Gateway pour les flux d'exploitation).

**25.1.3** Le titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

**25.1.4** En cas d'interconnexion des SI de l'acheteur et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures mise à disposition par l'acheteur (bastion SSL, API Gateway authentifiée) dans le respect du cadre technique et des règles de sécurité de l'acheteur.

**25.1.5** Pour chaque interconnexion, les éléments suivants seront définis par le titulaire au niveau des dispositifs d'accès de l'acheteur :

- Les flux et protocoles utilisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- Les modalités d'authentification : authentification par mot de passe, double-authentification forte ou par certificat ;
- Les modalités de chiffrement des échanges : le chiffrement des flux transitant sur Internet est requis ;
- les exigences spécifiques de traçabilité des accès ;

- Les moyens de sécurité supplémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif…

## Article 26

*Protection des données personnelles*

**26.1.1** Les exigences relatives à la protection des données personnelles sont définies dans l'article 5.2 du CCAG-TIC.

**26.1.2** Quand le CCP l'exige, le téléservice mettra à disposition des utilisateurs et administrateurs les moyens de régulation et de conformité au RGPD, a minima :

- Acceptation des dispositifs de traces (cookies) nécessaire au fonctionnement du téléservice. Les cookies tiers sont interdits,
- Acceptation de la politique de confidentialité et usage des données personnelles,
- Moyens de contacts du DPO de l'acheteur,
- Dispositifs d'exportation en format lisible de l'ensemble des données personnelles unitaires, archivage et suppression.

# Chapitre. 7e. **GLOSSAIRE**

| Acronyme / mot | Définition | Lien |
|---|---|---|
| AgentConnect | | https://agentconnect.gouv.fr/ |
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information | https://www.ssi.gouv.fr/ |
| API | Application Programming Interface (Interface de programmation d'application) | https://www.cnil.fr/fr/definition/interface-de-programmation-dapplication-api |
| ARCEP | Autorité de régulation des communications électroniques des postes et de la distribution de la presse | https://www.arcep.fr/ |
| | Cartographie des SI – guide ANSSI | https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/ |
| CCAG | Cahier des Clauses Administratives Générales | |
| CCAG-TIC | Cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication ; publié par arrêté au JORF le 1er avril 2021 (NOR : ECOM2106875A) | https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043310689 |
| CCP | Cahier des Clauses Particulières | |
| CCTP | Cahier des Clauses Techniques Particulières | |
| CERTA | Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques | |
| CNIL | Commission Nationale de l'Informatique et des Libertés | https://www.cnil.fr |
| | Constructions reproductibles | https://reproducible-builds.org/ |
| DAO | Data Access Object (objet d'accès aux données) | |
| | Gestion sémantique de version | https://semver.org/lang/fr |
| GlobalStats | | https://gs.statcounter.com/browser-market-share/all/france/ |
| IaaS | Infrastructure as a service - Hébergement par l'acheteur | |
| IHM | Interface Homme-Machine – *typiquement des écrans de saisie* | |
| | Les 12 facteurs | https://12factor.net/fr/ |
| MVC | Modèle-Vue-Contrôleur – cf DAO | |
| ORM | Object-Relational-Mapping (Mapping objet-relationel) | |
| OWASP | Open Web Application Security Project | |
| PaaS | Platform as a Service – hébergement par le titulaire (cas de sous-traitance de l'hébergement) | |
| PAMS | Prestataires d'administration et de maintenances sécurisé | https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf du 16/10/2022 |

| | | |
|---|---|---|
| PAS | Plan d'Assurance Sécurité | |
| PDF | Portable Document Format | |
| PSSI | Politique de Sécurité des Systèmes d'Information | PSSI-E : https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/ |
| Recette | | |
| RGAA | Référentiel Général d'Amélioration de l'Accessibilité | https://accessibilite.numerique.gouv.fr |
| RGESN | Référentiel Général d'Ecoconception de services numériques | https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/ |
| RGI | Règlement Général d'Interopérabilité (DINUM) | https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf |
| RGPD | Règlement Général sur la Protection des Données | https://www.cnil.fr/fr/reglement-europeen-protection-donnees |
| RGS | Règlement Général de Sécurité | v2 : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/ |
| SaaS | Software as a Service – hébergement par le titulaire | |
| Référentiel SecNumCloud | Référentiel d'exigences pour les prestataires de services d'informatique en nuage | V3.2 https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf |
| SIG | Service d'Information du Gouvernement | https://www.gouvernement.fr/marque-Etat |
| SSI | Sécurité des Systèmes d'Information | |
| TIC | Techniques de l'Information et de la Communication | |
| TU | Test Unitaire | |
| UML | Unified Modeling Language (langage de modélisation unifié) | |
| VA | Vérification d'Aptitude | |
| VSR | Vérification de Service Régulier | |
| XML | Extensible Markup Language (langage de balisage extensible) | |
| Zero Trust | Principe de défiance systématique | https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/ |