



Direction des systèmes d'information

MISE EN OEUVRE ET MAINTENANCE DU SITE CNRS.FR ET DE SITES SATELLITES

Cahier des Clauses Techniques Particulières

Livret 1/2 du CCTP n°25223

Accord cadre n°25.14.024

ANNEXE EXIGENCES TECHNIQUES

<p>Objet : Ce document décrit les exigences techniques, d'intégration dans le SI et de sécurité pour la mise en œuvre et la maintenance du futur site Portail CNRS.FR et de sites satellites du CNRS.</p>
--

SOMMAIRE

PRÉAMBULE	4
1 EXIGENCES LIÉES À L'HÉBERGEMENT, L'EXPLOITATION ET L'ADMINISTRATION.....	5
1.1 Hébergement.....	5
1.2 Environnements à mettre en œuvre.....	5
1.3 Architecture réseau.....	6
1.4 Architecture matérielle et logicielle.....	7
1.5 Services connexes.....	8
1.6 Intégration dans le SI.....	8
1.6.1 Accès et authentification des comptes utilisateurs.....	8
1.6.2 Accès et authentification des comptes administrateurs.....	9
1.7 Sauvegarde.....	10
1.8 Supervision.....	10
1.9 Chiffrement.....	11
1.10 Niveaux de service.....	12
1.11 Exigences en matière de plan de reprise d'activité (PRA).....	12
2 EXIGENCES LIÉES AUX DEVELOPPEMENTS ET À LA TMA.....	13
2.1 Conformités réglementaires.....	13
2.1.1 Politique Générale de Sécurité des systèmes d'Information.....	13
2.1.2 Protection des données à caractère personnel (DCP).....	14
2.1.3 Accessibilité numérique.....	14
2.1.4 Éco-conception.....	16
2.2 Principes d'urbanisation et d'intégration dans le SI.....	17
2.2.1 Principes généraux.....	17
2.2.2 Principes d'échanges.....	18
2.2.3 Plateformes transverses et services proposés.....	18
2.2.4 Prise en compte des changements de l'organisation structurelle du CNRS.....	19
2.2.5 Interopérabilité.....	19
2.3 Exigences d'intégration dans les SI.....	20
2.3.1 Répartition fonctionnelle.....	20
2.3.2 Echanges de données.....	20
2.3.3 Authentification, comptes utilisateurs.....	22
2.4 Exigences techniques.....	23
2.4.1 Choix du CMS.....	23
2.4.2 Eléments techniques structurant.....	24
2.4.3 Services d'infrastructure.....	24
2.4.4 Architecture applicative.....	26
2.4.5 Base de données.....	33
2.4.6 Engagements de qualité de service pour l'application.....	33
2.5 Exigences de sécurité.....	35
2.6 Exigences d'ergonomie-graphisme.....	35
2.6.1 Charte graphique.....	36
2.6.2 UX/UI et règles d'ergonomie.....	37
3 POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION (PSSI).....	39
3.1 Processus de Gestion de la sécurité.....	39
3.2 PSSI et déclinaison PAS (Plan d'Assurance Sécurité).....	39
3.3 Sensibilité des données.....	40
3.4 Organisation de la Sécurité des Systèmes d'Information (SSI).....	40
3.5 Relations avec les tiers.....	41
3.6 Processus de Gestion des incidents de sécurité.....	41
3.7 Dispositif de sécurité physique et environnementale.....	42

3.8	Contrôle des accès logiques	42
3.9	Interconnexion site titulaire et CNRS	43
3.10	Contrôle et conformité	43
3.11	Exigences liées aux développements	44
3.11.1	Auditabilité	45
3.11.2	Gestion des modules Drupal	46
4	PROTECTION DES DONNÉES À CARACTERE PERSONNEL (RGPD)	47
4.1	Définitions	47
4.2	Politique de protection des données personnelles au CNRS	47
4.3	Organisation de la protection des données	48
4.4	Politique de protection des données personnelles du titulaire	49
4.4.1	Registre des traitements	49
4.4.2	Formation des personnels	49
4.4.3	Confidentialité	49
4.5	Traitement des demandes d'accès aux données	50
4.6	Recours à des sous- traitants	50
4.7	Durée de conservation des données et archivage	50
4.8	Destruction, réversibilité	51
4.9	Analyse d'impact sur la vie privée	51
4.10	Exigences de sécurité	51
4.11	Traitement des incidents impactant les données à caractère personnel	52
4.12	Audit	52
4.13	Coopération avec les autorités de contrôle	52
5	ANNEXES	54
5.1	Glossaire	54

PRÉAMBULE

Les exigences techniques vis-à-vis du titulaire sont décrites dans les différents documents du Cahier des clauses techniques particulières (CCTP) dans des tableaux de la forme ci-dessous. La référence est composée de trois ou quatre lettres définissant le groupe d'exigences (cf. « **Référence des exigences** » ci-dessous) et de trois chiffres (pas nécessairement consécutifs). Les exigences sont classées selon trois niveaux :

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

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

Référence des exigences techniques :

Référence	Groupe d'exigence
ADM	Authentification des comptes administrateurs
AUTH	Authentification des comptes utilisateurs
BDD	Base de données
CON	Services connexes
DCP	Protection des données
DEV	Développement
ECH	Echange de données
ENV	Environnements
ERG	Ergonomie, graphisme
HAB	Habilitations
HEB	Hébergement
INF	Infrastructure
INT	Intégration dans le SI
MAT	Architecture matérielle et logicielle
OUT	Outillage
REGL	Conformité réglementaire
RES	Architecture réseau
SAV	Sauvegarde
SEC	Mesure et clauses de sécurité
SUP	Supervision
SSI	Sécurité des systèmes d'information
URB	Urbanisation

1 EXIGENCES LIÉES À L'HÉBERGEMENT, L'EXPLOITATION ET L'ADMINISTRATION

Ce chapitre présente les exigences d'infrastructure cible et services associés pour la nouvelle plateforme à mettre en place par le titulaire du présent marché.

1.1 HÉBERGEMENT

La future solution sera hébergée sur **un cloud privé** (IaaS) en dual datacenter, fourni par la personne publique. L'hébergeur apporte l'infrastructure matérielle.

Le titulaire prend en charge la définition de l'architecture de la solution (serveurs, réseau, stockage, dimensionnement, etc.) et sa mise en œuvre (installation, configuration, supervision, etc.). Tous les composants devront pouvoir ainsi fonctionner de façon optimale sur des environnements virtualisés.

Le RACI entre le titulaire du présent marché qui réalisera le MCO et l'hébergeur choisi par le CNRS est décrit au § 2.1.2.3 du document « CNRS.fr_CCTP-Livret2 ».

Référence	Libellé exigence	Priorité
HEB_001	Le traitement et la conservation des données du CNRS garantissent leur isolation vis-à-vis des données du titulaire et de celles des autres clients. L'intégrité et la confidentialité des données du CNRS sont garanties à tout moment. Le CNRS est particulièrement attentif à la qualité de la réponse permettant de garantir cette ségrégation.	0
HEB_002	Le CNRS exige que l'intégralité des fonctionnalités du service soit accessible au travers des navigateurs du marché dont la liste est fournie en annexe ("Cadre de cohérence technique versions cibles").	0

1.2 ENVIRONNEMENTS À METTRE EN ŒUVRE

Le titulaire crée, administre, exploite et maintient tous les environnements du périmètre applicatif et technique qu'il implémente sur l'hébergement IaaS fourni par le CNRS, en concertation avec le CNRS. Le titulaire assure notamment les activités suivantes pendant toute la durée de l'accord-cadre :

- la maintenance et la remise à niveau (ex : installation des sources et chargement de données, des jeux de tests, rafraîchissement d'environnements, application de patches et montées de version...) ;
- la gestion des profils et des accès des utilisateurs (du titulaire, du CNRS et des tiers légitimes le cas échéant) dans les environnements de son ressort ;
- la documentation associée.

Les prestations d'exploitation/administration et de TMA faisant l'objet d'un même marché, le titulaire doit proposer dans son offre une architecture disposant à minima de :

- Un environnement de Production :
 - destiné aux utilisateurs uniquement
 - Seule l'équipe d'exploitation/hébergement du titulaire à accès aux serveurs
- Deux environnements hors production destinés aux équipes projet du CNRS :
 - Un environnement de préproduction, copie de production sans données à caractère personnel
 - Un environnement de recette
 - permettant de valider les installations applicatives
 - permettant d'effectuer les vérifications fonctionnelles des évolutions et de non régression
 - Seule l'équipe d'exploitation/hébergement du titulaire à accès aux serveurs
- Tout autre composant ou environnement nécessaire aux équipes du titulaire pour :
 - développer les évolutions et les corrections demandées

- intégrer les divers composants dans des packages d'installation
- rédiger les manuels d'installation destinés à l'équipe d'exploitation
- effectuer des analyses et des investigations dans un contexte représentatif.

L'hébergement et la fourniture de ces autres composants est à la charge du titulaire.

Référence	Libellé exigence	Priorité
ENV_001	Le titulaire fournit et opère : <ul style="list-style-type: none"> - un environnement de production - le ou les environnements « hors production » dédiés à la validation des évolutions et à la non régression en amont de leur installation et implémentation en production. Ce/Ces environnements sont totalement étanches avec la production. Le titulaire ne copie dans ces environnements aucune donnée à caractère personnel du CNRS, en particulier issue de la production. Si le titulaire devait déployer des mécanismes d'anonymisation, ceux-ci seraient soumis préalablement à la validation explicite du CNRS ; - tout autre composant ou environnement nécessaire aux équipes du titulaire pour développer, intégrer les modifications et préparer les installations. 	0
ENV_002	Le titulaire définit avec l'approbation du CNRS le plan d'organisation, d'autorisation d'accès et de responsabilité sur les différents environnements fournis et pour les différents services.	0
ENV_003	Le CNRS demeure le seul et unique décisionnaire final concernant les autorisations d'accès y compris des tiers légitimes pour l'accès aux serveurs et à la centrale d'administration des environnements hors production à destination des équipes projet CNRS.	0
ENV_004	Les environnements du titulaire (postes de travail et serveurs) respectent les mêmes exigences de sécurité que les environnements à destination du CNRS	0

1.3 ARCHITECTURE RÉSEAU

La connectivité internet est fourni par l'hébergeur via deux liaisons (compatibles avec les protocoles IPv4 et IPv6) indépendantes et permanentes, une principale et une de secours.

Le débit des deux liaisons au démarrage du projet est de 1Gbps symétrique dédiés et pourra évoluer jusqu'à 10Gbps symétrique.

Référence	Libellé exigence	Priorité
RES-001	Le titulaire met en place un VPN IPSEC site à site, entre la solution et le centre serveur du CNRS pour consommer les webservices nécessaires	0
RES-002	Le service mis en place devra pouvoir absorber le débit réseau tout au long du marché	0
RES_003	Les accès internet sont filtrés. Les politiques associées sont définies par le CNRS et implémentées par le titulaire. Les règles font l'objet d'une revue en comité sécurité. D'une manière générale, aucun composant interne n'a d'accès direct entrant ou sortant à Internet.	0
RES_004	Le titulaire définit l'architecture logique du réseau local hébergeant le service et la décrit en incluant les briques techniques de service qui sont implantées (antivirus, antispam, CMDB, sauvegardes...).	0
RES_005	Tout au long du marché, le titulaire fournit au CNRS une matrice de flux interne et externe (trafic egress/ingress internet). Cette matrice de flux est implémentée sur les équipements de filtrage L4 à L7 de manière stricte sur les politiques de flux entrants et sortants.	0
RES_006	Tout au long du marché, le titulaire fournit au CNRS les schémas d'architecture de haut et bas niveau de la solution. Ces documents sont mis à jour à chaque changement. Les plans d'adressage IP détaillés sont également fournis et tenus à jour.	0

RES_007	<p>Le titulaire fournit et met en œuvre des dispositifs de filtrage des accès Internet sortants. Tous ces dispositifs assurent des ruptures protocolaires et sont hébergés dans au moins une zone de sécurité autonome (DMZ-OUT) en respect des recommandations de l'ANSSI</p> <p>L'ensemble des flux sortants initiés dans les zones logiques hébergées sont filtrés et passent par ces dispositifs qui répondent aux caractéristiques minimales suivantes :</p> <ul style="list-style-type: none"> - Implémentation d'une politique de sécurité où tout flux non explicitement autorisé est interdit, - Inspection des flux avec gestion des états (stateful) jusqu'au niveau OSI 4 <p>Pour les flux sortants de messagerie et les flux transportés par HTTP, l'inspection des paquets porte sur l'ensemble des couches du modèles OSI (jusqu'au niveau 7 – applicatif).</p>	0
RES_008	<p>Le titulaire fournit et met en œuvre des dispositifs de filtrage des accès Internet entrants. Tous ces dispositifs assurent des ruptures protocolaires et sont hébergés dans au moins une zone de sécurité autonome (DMZ-IN) en respect des recommandations de l'ANSSI</p> <p>Ces dispositifs répondent aux caractéristiques minimales suivantes :</p> <ul style="list-style-type: none"> - Gestion de plusieurs zones de sécurité, et de plusieurs politiques de filtrage par zone - Inspection des flux avec gestion des états (stateful) jusqu'au niveau OSI 7 - Déchiffrement à la volée des flux chiffrés pour permettre leur inspection sans perturbation notable des performances applicatives - Implémentation de règles de filtrage applicatif par application, permettant de s'assurer de la conformité des flux avec les normes protocolaires et avec les contenus légitimement attendus par les applications 	0
RES_09	Des éléments réseau filtrants assurent la ségrégation des flux internes à la plateforme en accord avec la segmentation du réseau. Seuls les flux nécessaires doivent être autorisés.	0
RES_010	Une micro-segmentation entre éléments d'un même réseau serait un plus.	1
RES_011	Tous les échanges vers et depuis Internet utilisent le protocole de chiffrement TLS dans ses versions non affectées par des vulnérabilités et respectent les contraintes du RGS (sauf avis contraire et transitoire du CNRS pour des raisons de compatibilité).	0

1.4 ARCHITECTURE MATÉRIELLE ET LOGICIELLE

L'architecture matérielle est fournie par l'hébergeur.

Référence	Libellé exigence	Priorité
MAT_001	<p>Tous les éléments logiciels mis en œuvre par le titulaire sont couverts par des contrats de maintenance souscrits auprès des éditeurs/constructeurs des solutions en accord avec les SLA demandés par le CNRS.</p> <p>Le titulaire maintient à jour les éléments logiciels de la solution, de sorte qu'à aucun moment, la solution ne se trouve sans support de son éditeur/constructeur.</p>	0
MAT_002	Les composants nécessaires à la solution sont utilisés dans les versions les plus récentes et dont la durée de support est la plus longue, ce qui implique des mises à jour régulières en conséquence, avec des calendriers de mise en œuvre avec accord du CNRS.	0
MAT_003	<p>Si une mise à jour provoque une indisponibilité du service :</p> <ul style="list-style-type: none"> - Le CNRS et le titulaire planifient l'opération, le CNRS pouvant imposer une réalisation en HNO - L'indisponibilité éventuelle due à ces opérations ne sera pas comptabilisée dans le calcul du taux de disponibilité du service 	0
MAT_004	Les mises à jour de sécurité de CVSS supérieur ou égal à 9 doivent être réalisées dans les 24 heures qui suivent leur publication suite à une analyse de risque à faire dans les 2h.	0
MAT_005	Les mises à jour de sécurité de CVSS compris entre 7.x et 8.x doivent être réalisées dans les 7 jours qui suivent leur publication.	0

MAT_006	Les mises à jour de sécurité de CVSS inférieur à 7 doivent être réalisées dans les 30 jours qui suivent leur publication.	0
MAT_007	Les mises à jour mineures sont installées au maximum 3 mois après leur publication	0
MAT_008	Les versions majeures doivent être installées au maximum dans les 12 mois suivant leur sortie sauf avis contraire du CNRS.	0
MAT_009	Le titulaire met en place et maintient une gestion des actifs matériels et logiciels de la plateforme permettant notamment le suivi des contrats de maintenance et de licences.	0
MAT_010	Tout matériel de stockage ayant contenu des données du CNRS ou des éléments de configuration est détruit ou reconditionné, conformément aux directives ANSSI.	0
MAT_011	Pour chacune des fonctionnalités demandées, le CNRS exige l'utilisation de produits qualifiés ou à minima certifiés par l'ANSSI lorsqu'ils existent.	0
MAT_012	Les technologies mises en œuvre par la plateforme respectent les RFC à l'état de l'art, notamment l'internationalisation...	0

1.5 SERVICES CONNEXES

Référence	Libellé exigence	Priorité
CON_001	Le CNRS fournit les entrées DNS publiques nécessaires au fonctionnement du service sur demande du titulaire.	0
CON_002	Le titulaire assure la gestion des DNS internes à la plateforme.	0
CON_003	Le titulaire implémente et maintient un service NTP permettant la synchronisation de l'horloge sur l'ensemble de ses équipements. La base de temps est fournie par le titulaire. Les serveurs dans les différents sites mis en œuvre doivent avoir la même base de temps et a minima des serveurs NTP de même stratum.	0
CON_004	Le titulaire implémente et maintient un service de PKI interne permettant de distribuer et gérer le cycle de vie des certificats de chiffrement/signature internes à la solution.	0
CON_005	Le titulaire implémente et maintient un relai SMTP permettant la redirection de l'envoi de mails vers le service SMTP du CNRS.	0
CON_006	Le CNRS exige la présence d'outils de protection contre les virus et logiciels malveillants sur tous les serveurs concernés par le transit dans les 2 sens de communication. La solution est mise à jour a minima quotidiennement.	0
CON_007	Le CNRS exige l'utilisation de produits hébergés sur la plateforme (on premise). A défaut, si aucune solution on premise n'est possible, une solution SaaS dans un hébergement cloud souverain peut être tolérée sur justification.	0
CON_008	Le titulaire implémente et maintient un service de fédération permettant de raccorder les Back-Office aux fournisseurs d'identité pris en charge par le CNRS ou RENATER (fédération d'identité Education Recherche), comprenant entre autres Janus et l'IDP du CNRS.	0

1.6 INTÉGRATION DANS LE SI

Référence	Libellé exigence	Priorité
INT_001	La plateforme mise en œuvre par le titulaire doit permettre de consommer les données extérieures : authentification, connexion aux web services référentiels, échanges via le système EAI du CNRS.	0

1.6.1 Accès et authentification des comptes utilisateurs

Les exigences de ce paragraphe concernent l'accès au backoffice par les différents acteurs CNRS (contributeurs, valideurs, équipes projet etc.).

Référence	Libellé exigence	Priorité
AUT_001	Les accès au backoffice (publication, modification de contenu, etc.) doivent se faire au travers d'une solution qualifiée ou à minima certifiée par l'ANSSI, de VPN Client authentifiée à 2 facteurs dans une configuration conforme aux recommandations de l'ANSSI. Les outils de backoffice ne doivent pas être exposés en dehors de ces accès VPN	0
AUT_002	La solution de VPN permet de gérer : <ul style="list-style-type: none"> - Le cycle de vie des utilisateurs - L'enrôlement des facteurs d'authentification - Les politiques de mot de passe - Se protéger contre les attaques par force brute - S'interfacer avec les systèmes de gestion des utilisateurs du CNRS Ce service respecte les exigences de souveraineté et d'indépendance aux ressources cloud/SaaS et est conforme aux recommandations de l'ANSSI	0
AUT_003	Si la solution de VPN le permet, l'authentification des utilisateurs s'appuie sur une authentification fédérée incluant les fournisseurs d'identité renforcés du CNRS : Janus+ et Janus+ UHPI. Dans le cas contraire, l'authentification des utilisateurs s'appuie à minima sur Janus et Janus UHPI.	0
AUT_004	Tous les accès utilisateurs sont obligatoirement authentifiés et doivent se faire via une DMZ.	0
AUT_005	Le CNRS doit pouvoir identifier et filtrer les accès en fonction du contexte de l'accès client : adresse IP, zone géographique, horaire. Le titulaire décrit comment il met en œuvre cette capacité de détection et de filtrage (interdiction d'accès en fonction de ces critères au choix paramétrable du CNRS).	0

1.6.2 Accès et authentification des comptes administrateurs

Les exigences de ce paragraphe concernent l'accès aux services d'administration (bastion, serveurs) de la plateforme pour l'équipe du titulaire.

Référence	Libellé exigence	Priorité
ADM_001	Les accès des administrateurs s'effectuent au travers d'une solution de VPN IPSEC qualifiée ou à minima certifiée par l'ANSSI de type site à site dans une configuration conforme aux recommandations de l'ANSSI.	0
ADM_002	L'authentification au service d'administration de la plateforme ne s'appuie pas sur le service SSO du CNRS mais sur son propre service local d'authentification. Ce service est donc fourni par le titulaire dans la solution et est de sa seule responsabilité.	0
ADM_003	Les moyens d'authentification (mot de passe, ...) et leur complexité (type et nombre de types de caractères, longueur...) devront pouvoir être modifiés en cours de contrat sur demande du CNRS.	0
ADM_004	La solution permet de paramétrer la durée de vie des mots de passe des utilisateurs et ainsi changer cette durée en cours de contrat.	0
ADM_005	Le CNRS exige une protection contre les tentatives d'attaque par « force brute » : au bout d'un nombre de tentatives d'authentifications infructueuses définie dans le PAS, l'accès au service est suspendu pour le client concerné pour une durée fixée et le compte utilisateur est verrouillé. Les administrateurs de la plateforme et le RSSI doivent être informés.	0
ADM_006	Le CNRS exige qu'une authentification multifacteurs (MFA) soit mise en œuvre pour les tâches d'administration, propose les protocoles à l'état de l'art du moment (OTP, WebAuthn, FIDO2...) et respecte leurs RFC. Ce service respecte les exigences de souveraineté et d'indépendance aux ressources cloud/SaaS.	0
ADM_007	Dans le cadre de la mise en œuvre, les modalités d'initialisation du service et de gestion de la première authentification sont à définir conjointement entre le CNRS et le titulaire (notamment pour les comptes de services, les comptes d'administration...).	0
ADM_008	Seuls les protocoles d'accès normalisés sont utilisables. Le CNRS se réserve le droit, sur simple demande du RSSI de bannir certains protocoles.	0

ADM_009	Pour les comptes disposant d'un mot de passe : une fonction de hachage conforme au Référentiel Général de Sécurité (https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs) est utilisée pour calculer l'empreinte des mots de passe.	0
----------------	--	---

1.7 SAUVEGARDE

Les outils et mécanismes de sauvegarde sont fournis dans le cadre de l'hébergement.

Les sauvegardes sont chiffrées.

Référence	Libellé exigence	Priorité
SAV_001	Le titulaire implémente et maintient les plans de sauvegarde permettant de répondre aux exigences de Niveaux de Service du CNRS en termes de PDMA applicable à la politique de sauvegarde et DMIA durée d'indisponibilité maximale admissible, telles que définies dans le document joint « CNRS.fr_CCTP-Livret2_Annexe_Niveaux_de_service.xls ».	0
SAV_002	Les supports de sauvegarde sont externalisés de manière régulière dans un emplacement connu par le CNRS, suffisamment distant du site principal pour résister à un désastre régional et sur le territoire français métropolitain.	0
SAV_003	Au démarrage de l'accord-cadre, les supports contenant les sauvegardes antérieures sont livrés déchiffrés au titulaire. Le titulaire applique le principe de chiffrement des supports externalisés (hors site) : - chiffrer les supports avant externalisation - chiffrer les supports déchiffrés mis à disposition par le CNRS - détruire les supports contenant les données non chiffrées conformément aux exigences de l'ANSSI	0
SAV_004	Le titulaire fournit tous les mois la synthèse des rapports de sauvegarde et des tests de restaurations de la période. Le CNRS peut demander à tout instant la visibilité des journaux de sauvegarde et de restauration.	0
SAV_005	Le plan de sauvegarde est à présenter par le titulaire. Le plan de sauvegarde est proposé par le titulaire et validé par le CNRS, dans le respect des SLA de disponibilité et d'intégrité des données, telles que définies dans le document joint « CNRS.fr_CCTP-Livret2_Annexe_Niveaux_de_service.xls ». Le CNRS peut, sur demande, obtenir une sauvegarde complète des données de la plateforme.	0
SAV_006	La durée de rétention des sauvegardes sera de 12 mois selon la politique de sauvegarde définie avec le CNRS, mais pourra être modifiée par le CNRS en cas de nouvelle contrainte gouvernementale.	0
SAV_007	Le plan de sauvegarde décrit les mécanismes et procédures de restauration « sur demande » de sites.	0

1.8 SUPERVISION

Ces exigences concernent le système de supervision matérielle, système et réseau, ainsi que la gestion des logs applicatifs (accès aux fonctions d'administration de l'environnement de vérification...).

Référence	Libellé exigence	Priorité
SUP_001	La solution technique de supervision proposée et maintenue par le titulaire, est à l'état de l'art dans ce qui se fait sur le domaine.	0
SUP_002	Le titulaire est responsable de la fourniture des moyens de supervision, de leur exploitation et la fourniture au CNRS d'un moyen de consulter l'état de la supervision.	0
SUP_003	Le CNRS dispose de manière périodique et automatique de métriques sur l'état de santé du service applicatif (par exemple le taux d'occupation du stockage, le taux d'usage des instances...).	0

SUP_004	L'application fournit des fichiers de logs avec un formatage facilitant leur analyse automatique ainsi qu'une capacité d'export vers un collecteur de logs techniques centralisé	0
SUP_005	Le titulaire s'assure de l'adéquation de la supervision avec les modifications qu'il apporte à la plateforme.	0
SUP_006	Le CNRS exige que le système de journalisation mis en place par le titulaire respecte les recommandations de l'ANSSI.	0
SUP_007	Le titulaire documente et met en œuvre une politique de journalisation incluant au minimum les éléments suivants : <ul style="list-style-type: none"> - La liste des sources de collecte - La liste des événements à journaliser par source - L'objet de la journalisation par événement - La fréquence de la collecte et base de temps utilisée - La durée de rétention locale et centralisée - Les mesures de protection des journaux (dont chiffrement et duplication) - La localisation des journaux 	0
SUP_008	Le titulaire génère, collecte et donne accès au CNRS aux événements suivants : <ul style="list-style-type: none"> - Les activités des utilisateurs liées à la sécurité de l'information - La modification des droits d'accès dans le périmètre de sa responsabilité - Les événements issus des mécanismes de lutte contre les codes malveillants - Les exceptions - Les défaillances - Tout autre événement lié à la sécurité de l'information 	0
SUP_009	Le titulaire conserve les événements issus de la journalisation pendant une durée minimale de douze mois glissants sous réserve du respect des exigences légales et réglementaires. Par défaut, tout événement est tracé, sauf exemption dûment validée par le CNRS. Les informations contenues dans la trace sont a minima définies supra mais peuvent être augmentées. L'objectif est la recherche d'imputabilité des actions légitimes ou non des utilisateurs et administrateurs.	0
SUP_010	Le titulaire opère un service dédié de consultation des événements journalisés permettant des fonctions de recherche avancée, de filtrage des événements et de corrélation, hébergé par le titulaire sur l'infrastructure IaaS.	0
SUP_011	La communication des traces sur injonction d'une autorité, française ou étrangère, ne peut être réalisée que : <ul style="list-style-type: none"> - sur information préalable du CNRS dans le cas d'une autorité française, - sur autorisation préalable du CNRS dans le cas d'une autorité étrangère. 	0

1.9 CHIFFREMENT

Référence	Libellé exigence	Priorité
SEC_001	Les données stockées sont chiffrées au repos. Les algorithmes utilisés sont au niveau de robustesse du Référentiel Général de Sécurité (RGS annexes B).	0
SEC_002	Hormis les données chiffrées par les utilisateurs, tout chiffrement d'objets implique la mise en œuvre de procédures permettant de restituer en toutes circonstances les données en clair en cas de perte du secret permettant de les déchiffrer. Le titulaire tient à disposition du CNRS, à tout moment, les secrets nécessaires au recouvrement de ses données, nécessaires à la mise en œuvre des procédures de réversibilité de la prestation	0
SEC_003	Le niveau de robustesse des algorithmes de chiffrement et de hachage utilisés est conforme aux dispositions en vigueur (à date : RGS v2.x annexes B en particulier, règlement eIDAS). Tout algorithme déprécié ou moins robuste est remplacé.	0

1.10 NIVEAUX DE SERVICE

L'architecture technique de la solution ainsi que le dispositif humain déployé devront permettre l'atteinte des niveaux de service décrits dans le document joint « CNRS.fr_CCTP-Livret2_Annexe_Niveaux_de_service.xls ».

1.11 EXIGENCES EN MATIÈRE DE PLAN DE REPRISE D'ACTIVITÉ (PRA)

L'architecture technique et applicative proposée par le titulaire devra permettre de mettre en œuvre un plan de reprise informatique en cas de sinistre majeur (type incendie, dégât des eaux...) se produisant sur le datacenter principal hébergeant la solution. La personne publique prévoit de mettre à disposition un hébergement avec une stratégie « dual datacenter ».

Dans un contexte de Plan de Reprise d'Activité (qui serait déclenché en cas de sinistre majeur), les niveaux de service requis (environnement de production) sont décrits dans le document joint « CNRS.fr_CCTP-Livret2_Annexe_Niveaux_de_service.xls ».

Le titulaire réalise un test annuel complet ou partiel du PRA et informe au préalable le CNRS de la date du test afin que ce dernier puisse y assister s'il le souhaite. Le titulaire transmet le procès-verbal et les résultats du test au CNRS.

Le titulaire réalise une revue annuelle du PRA en fonction des résultats du test, des évolutions techniques et des évolutions du contexte, puis partage les résultats de cette revue ainsi que la liste des éventuelles actions correctives / évolutives identifiées avec le CNRS.

2 EXIGENCES LIÉES AUX DEVELOPPEMENTS ET À LA TMA

Ce chapitre donne les exigences applicables à tout nouveau développement

2.1 CONFORMITÉS RÉGLEMENTAIRES

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

Référence	Libellé exigence	Priorité
REGL_001	L'objectif de conformité au référentiel RGS (Référentiel général Sécurité) est poursuivi : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs	2
REGL_002	Les applications sont mises en œuvre conformément au RGAA (Référentiel général d'amélioration de l'accessibilité) : https://accessibilite.numerique.gouv.fr/	0
REGL_003	Les solutions applicatives sont mises en œuvre conformément au RGESE (Référentiel général d'écoconception de services numériques) : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/	1
REGL_004	L'objectif de conformité au référentiel RGI (Référentiel général Interopérabilité) est poursuivi : https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/	2
REGL_005	La page d'accueil de la solution permet d'accéder aux mentions légales : licence d'utilisation du logiciel, point de contact éditorial et technique, éventuelles mentions légales réglementaires concernant les données à caractère personnel, l'utilisation des cookies.	0
REGL_006	La gestion des cookies est conforme à la réglementation en vigueur. La solution permet d'afficher la liste des cookies nécessaires à son fonctionnement et la manière de les supprimer dans les navigateurs supportés.	0
REGL_007	La solution s'interface avec ou gère une plateforme de gestion des consentements (consent management platform) permettant de débrayer le positionnement des cookies non essentiels.	1

2.1.1 Politique Générale de Sécurité des systèmes d'Information

Concernant les aspects sécurité, les objectifs de la Politique Générale de Sécurité des systèmes d'Information (PGSI¹) du CNRS sont les suivants :

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

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

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

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

- Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
- L'application de cette politique est contrôlée.

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

Référence	Libellé exigence	Priorité
REGL_008	<p>Le titulaire se conforme au cadre réglementaire applicable en termes de SSI, à savoir (de façon non exhaustive) :</p> <ul style="list-style-type: none"> - Les annexes techniques du Référentiel Général de Sécurité (RGS) - La Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E) - L'instruction interministérielle 901 (II 901) portant sur les informations sensibles marquées « diffusion restreinte » - La PSSI du CNRS (PSSI-C). <p>RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs PSSI-E : https://www.legifrance.gouv.fr/circulaire/id/38641 II 901 : https://cyber.gouv.fr/instruction-interministerielle-n901 PSSI-C : document non public, disponible sur demande</p>	0
REGL_009	Les configurations des matériels (inclus les solutions appliances les équipements réseau) et des systèmes (inclus les OS, les firmwares et les hyperviseurs) embarqués dans la solution sont durcies.	0

2.1.2 Protection des données à caractère personnel (DCP)

Référence	Libellé exigence	Priorité
REGL_010	<p>Le titulaire se conforme aux réglementations applicables en termes de protection des données à caractère personnel :</p> <ul style="list-style-type: none"> - Règlement n°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 (RGPD), - Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et textes pris pour son application. - Les traitements sont également réalisés en conformité avec toute délibération et recommandation de la Commission nationale de l'informatique et des libertés (CNIL). 	0

Les exigences CNRS en matière de DCP sont décrites dans le chapitre 4 Protection des données à caractère personnel.

2.1.3 Accessibilité numérique

Dans le cadre du développement du portail cnrs.fr et de ses sites satellites, le titulaire est tenu de respecter les obligations légales françaises en matière d'accessibilité numérique, conformément à l'article 47 de la loi n° 2005-102 du 11 février 2005, au décret n° 2019-768 du 24 juillet 2019, et au Référentiel Général d'Amélioration de l'Accessibilité (RGAA) version 4.1.2, basé sur les WCAG 2. Le respect du RGAA est requis pour les sites, et une déclaration d'accessibilité spécifique est produite pour le portail principal et chaque site satellite.

1. Conformité au RGAA 4.1.2

- **Taux de conformité RGAA** : Le titulaire garantit que l'ensemble des pages des sites atteignent un taux conforme aux critères du RGAA 4.1.2, sauf dérogations exceptionnelles dûment justifiées (voir section 4).
- **Périmètre d'application** : Cette exigence s'applique à toutes les pages, fonctionnalités, et contenus (interfaces, formulaires, contenus multimédias, contenus dynamiques) du portail principal et de chaque site satellite.
- **Standards techniques** : Le code HTML, CSS, et JavaScript est conforme aux standards W3C (HTML5, CSS3) et compatible avec les technologies d'assistance (lecteurs d'écran comme NVDA, JAWS, VoiceOver, et afficheurs braille).

2. Déclaration d'accessibilité par site

- **Rédaction et publication** : Le titulaire fournit une déclaration d'accessibilité distincte pour le portail web principal et pour chaque site satellite, conforme au modèle du RGAA 4.1.2. Chaque déclaration est publiée sur le site concerné, dans une section facilement accessible (par exemple, en pied de page ou dans une rubrique dédiée). Chaque déclaration inclut :
 - Une affirmation explicite du taux de conformité sur les pages échantillonnées du site concerné, ou une justification claire des écarts en cas de non-conformité partielle.
 - Une liste des éventuelles non-conformités spécifiques au site, avec explications et justifications.
 - Un lien vers un formulaire de contact dédié permettant aux utilisateurs de signaler des problèmes d'accessibilité pour le site concerné. L'adresse courriel de contact sera fournie par le CNRS.
 - Une mention de la possibilité de saisir le Défenseur des droits en cas de non-réponse à une réclamation dans un délai d'un mois.
- **Accessibilité des déclarations** : Chaque déclaration est rédigée dans un format accessible, compatible avec les technologies d'assistance, et disponible en lecture facile si pertinent.
- **Centralisation** : Une page centralisée sur le portail principal liste les liens vers le Schéma Pluriannuel Accessibilité Numérique du CNRS, les annexes et le plan d'action de l'année en cours. Ces documents sont fournis par le CNRS.

3. Audit et validation

- **Audit par site** : Le titulaire réalise un audit d'accessibilité distinct pour le portail principal et chaque site satellite, conformément à la méthodologie RGAA 4.1.2. Chaque audit couvre un échantillon représentatif de pages et de fonctionnalités spécifiques au site, démontrant le taux de conformité RGAA sur les pages échantillonnées.
- **Rapport d'audit par site** : Pour chaque site (portail principal et sites satellites), le titulaire fournit un rapport détaillé incluant :
 - Le taux de conformité.
 - La liste des pages auditées et des critères RGAA vérifiés.
 - Les résultats des tests avec les principales technologies d'assistance (NVDA, JAWS, VoiceOver, etc.).
 - Une confirmation que toutes les non-conformités éventuelles ont été corrigées avant livraison.
- **Tests utilisateurs** : Des tests avec des utilisateurs en situation de handicap (visuel, auditif, moteur, cognitif) sont organisés pour chaque site afin de valider l'accessibilité pratique et l'ergonomie des interfaces.
- **Outils d'évaluation** : Les audits combinent des outils automatiques (par exemple, WAVE, Axe) et une vérification manuelle pour garantir l'exactitude des résultats.

4. Dérogations exceptionnelles

- **Charge disproportionnée** : Toute dérogation pour cause de charge disproportionnée est spécifique à un site donné, justifiée par une analyse détaillée (coût, impact, alternatives possibles), et soumise à l'approbation préalable du maître d'ouvrage. Cette justification est incluse dans la déclaration d'accessibilité du site concerné.
- **Incompatibilité technique** : Toute dérogation pour incompatibilité technique est documentée avec des preuves techniques et un plan de contournement ou de correction future, spécifique au site.
- **Validation des dérogations** : Les dérogations sont validées par le maître d'ouvrage et conformes aux exigences du RGAA 4.1.2.

5. Plan d'action en cas de non-conformité

- **Correction immédiate par site** : Si des non-conformités sont identifiées lors des audits, le titulaire les corrige dans un délai défini par le maître d'ouvrage, afin d'atteindre le taux de conformité RGAA sur les pages échantillonnées de chaque site.
- **Plan d'action par site** : Un plan d'action spécifique à chaque site est fourni, incluant :
 - La liste des non-conformités identifiées pour le site.
 - Les mesures correctives prévues.
 - Un calendrier précis pour les corrections.
- **Vérification post-correction** : Un audit complémentaire par site est réalisé pour confirmer la conformité RGAA après correction.

6. Maintenance et suivi

- **Conformité continue** : Le titulaire garantit que toute mise à jour ou évolution du portail principal ou d'un site satellite maintient un taux de conformité de RGAA sur les pages échantillonnées auditées.

- **Formation** : Le titulaire fournit une formation ou une documentation détaillée aux équipes internes du maître d'ouvrage sur les bonnes pratiques d'accessibilité pour la gestion des contenus de chaque site.
- **Mise à jour des déclarations** : Chaque déclaration d'accessibilité est actualisée selon la périodicité requise dans le RGAA ou à chaque modification majeure du site concerné, confirmant le maintien du taux de conformité RGAA.

7. Responsabilité légale

- **Conformité légale** : Le titulaire est pleinement responsable du respect des obligations légales fixées par l'article 47 de la loi n° 2005-102, le décret n° 2019-768, et le RGAA 4.1.2 pour chaque site. Tout manquement peut entraîner des sanctions administratives ou judiciaires, notamment via le Défenseur des droits.
- **Pénalités contractuelles** : En cas de non-atteinte du taux de conformité de RGAA sur les pages échantillonnées d'un site, sauf dérogations validées, le titulaire doit prendre en charge les coûts de mise en conformité.
- **Documentation** : Le titulaire fournit une documentation complète pour chaque site, prouvant la conformité RGAA, incluant les rapports d'audit, les justificatifs de dérogations, et les plans d'action correctifs.

8. Références réglementaires

- **Le titulaire se conforme aux textes suivants** :
 - Article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.
 - Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne.
 - Référentiel Général d'Amélioration de l'Accessibilité (RGAA) version 4.1.2, disponible sur le site de la DINUM (Direction interministérielle du numérique).
- Les WCAG 2 (Web Content Accessibility Guidelines) sont utilisées comme base technique pour la mise en œuvre.

9. Livrables attendus

- Une déclaration d'accessibilité distincte pour le portail principal et chaque site satellite, publiée et indiquant le taux de conformité sur les pages échantillonnées ou justifiant toute dérogation.
- Un rapport d'audit initial par site, démontrant la conformité RGAA des pages échantillonnées.
- Des rapports d'audit complémentaires pour chaque phase de mise à jour ou évolution d'un site.
- Un plan d'action spécifique par site pour la correction des non-conformités, si applicable.
- Une documentation technique détaillant les mesures prises pour assurer l'accessibilité de chaque site (code, tests, outils utilisés).
- Une formation ou documentation pour les équipes internes sur la gestion de l'accessibilité pour chaque site.

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

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

2.1.4 Éco-conception

Le CNRS a pour ambition de mettre à disposition de ses utilisateurs des applications conçues dans une démarche écoresponsable afin de réduire au maximum ses émissions de gaz à effet de serre (GES) et ses besoins en ressources énergétiques. Les principaux leviers sont listés ci-dessous :

1. CMS et composants :

- Favoriser la mutualisation et l'utilisation de briques transverses ;
- Choisir des composants libres et pérennes, reconnus et maintenus par la communauté ;

2. Optimisation du code et des ressources :

- Le code HTML, CSS et JavaScript devra être conforme aux standards W3C.
- Limiter les solutions proposées dans les applications aux besoins réels des utilisateurs (frugalité des besoins) ;
- Privilégier des solutions techniques simples et peu coûteuses vis-à-vis des données échangées (ex : poids des pages, formats utilisés ...) ;

- Dans le cadre de la gestion des fichiers stockés sur la plateforme, intégrer la possibilité pour l'utilisateur de visualiser les informations dans le navigateur en évitant les téléchargements, d'obtenir un lien de visualisation plutôt que de téléchargement, puis un lien de téléchargement pour intégration ou vignette quand c'est possible.

3. Design & Performance des pages :

- Faire du Responsive Design avec l'idée de limiter la bande passante
- Proposer une mise en cache efficace
- Optimiser le poids des pages (poids du code, poids des images -compression .-, adaptation à la résolution, utiliser la pagination plutôt que le défilement infini, Compresser les images en WebP, AVIF et JPEG optimisées, selon compatibilité des navigateurs. Éviter les GIFS et plutôt utiliser des animations en CSS.)
- Une compression automatique (sans perte) sera mise en œuvre sur les images. Qu'il s'agisse d'un média uploadé par un contributeur, ou d'un média récupéré de l'extérieur (flux RSS, API, etc.).
- Le nombre de requêtes HTTP sera minimisé par le regroupement et la minification des ressources.

4. Données :

- Dimensionner de façon juste les infrastructures ;
- Accroître la durée de vie des applications en améliorant leur urbanisation et leur maintenance ;
- Proposer des stratégies de gestion du cycle de vie des données pour limiter le stockage inutile

5. Suivi et mesure de l'impact :

- Un audit initial de performance environnementale (EcoIndex, Lighthouse ou équivalent) sera fourni à la livraison
- Proposer des outils permettant de suivre la performance environnementale sur la durée, à l'aide de rapports. Green-it CLI est une piste. Il est possible de générer des rapports, sur des parcours précis, et d'automatiser en partie. Attention, les solutions tiers propriétaires, peuvent ne pas convenir au regard du coût budgétaire et environnemental que cela peut engendrer.
- Améliorer la sécurisation des applicatifs pour limiter l'occurrence des incidents et leur coût de gestion.
- Proposer une série d'indicateurs de mesure pour le pilotage
- Faire des recommandations pour maintenir une démarche éco-responsable lors des évolutions futures

Le titulaire respecte au mieux ces grands principes qui doivent guider ses choix de conception.

Ces exigences peuvent être complétées par les préconisations du chapitre « Services numériques » du guide « Bonnes pratiques numérique responsable pour les organisations » de la Direction Interministérielle du Numérique (DINUM) :

<https://ecoresponsable.numerique.gouv.fr/docs/2023/guide-de-bonnes-pratiques-numerique-responsable-version-1.pdf>.

Le Titulaire décrit dans son offre ses engagements en la matière et les moyens qu'il entend mettre en œuvre pour les satisfaire.

2.2 PRINCIPES D'URBANISATION ET D'INTÉGRATION DANS LE SI

2.2.1 Principes généraux

La démarche d'urbanisation mise en œuvre à la DSI du CNRS doit accompagner, faciliter et maîtriser la transformation continue et progressive du SI en le rendant de plus en plus agile et en assurant sa pérennité pour en tirer le maximum de plus-value, en cohérence avec les orientations stratégiques, métiers et opérationnelles de l'organisme.

Cette démarche doit aider l'évolution du SI par une optimisation de l'existant, tournée vers les objectifs suivants :

- capitaliser sur les socles existants ;
- poursuivre l'intégration des différents systèmes dans l'optique d'une gestion modernisée ;
- garantir la fiabilité des données de référence dans le système d'information global.

Plus particulièrement, 4 grands principes sont mis en avant par la démarche d'urbanisation et d'intégration dans les SI :

1. Principe de cohérence forte pour aider à répartir les contours fonctionnels et informationnels entre les applications du SI dans le but d'éviter toute redondance fonctionnelle et de limiter les flux entre applications participant au même processus métier. Un modèle informationnel et un modèle des processus métier sont fortement recommandés, voire attendus, pour aider à ces choix de répartition applicative ;
2. Principe de couplage faible entre applications pour réduire les dépendances entre applications et ainsi limiter les impacts sur le SI en cas d'évolution d'une partie de ce SI ;
3. Développer l'utilisation de briques numériques, fonctionnelles et/ou applicatives communes et mutualisées dans une logique de plateformes transverses ;
4. Prendre en compte la dimension « laboratoire » et ainsi découpler de façon modulaire (modules applicatifs disjoints) autant que faire se peut les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans la perspective de futures mutualisations potentielles des fonctionnalités « Laboratoire » et d'éventuelle répartition dans des SI distincts des fonctionnalités « Etablissement » et « Laboratoire » ; le tout en cohérence avec les actions parallèles éventuelles sur les mêmes sujets par les SI des établissements partenaires du CNRS.

L'architecture proposée par le titulaire est soumise à la validation de la DSI du CNRS.

2.2.2 Principes d'échanges

Pour mettre en œuvre le principe de couplage faible, des protocoles d'échanges sont établis, préconisant l'utilisation de :

- systèmes d'intermédiation (cf. § 2.2.3) pour éviter les échanges point à point entre deux applications en procédant par $\frac{1}{2}$ flux via ces systèmes d'intermédiation) pour éviter les échanges point à point entre deux applications en procédant par $\frac{1}{2}$ flux via ces systèmes d'intermédiation ;
- formats d'échange communs sous la forme de format pivot par objet métier échangé. Le format pivot, indépendant des applications et de leur modèle de données, est une représentation partagée et intrinsèque d'un objet (métier ou technique), tenant compte de l'ensemble de ses cas d'usages. Il précise aussi les référentiels et nomenclatures communs et partagés à utiliser éventuellement pour ses attributs ;
- fonctions d'intégration (ou services applicatifs) de ces formats pivots dans le cadre des flux entrants ;
- fonctions d'exposition (ou services applicatifs) des informations vers ces formats pivots dans le cadre des flux sortants.

Ces principes s'appliquent aussi bien aux échanges de données et informations internes au SI qu'aux échanges avec l'extérieur.

2.2.3 Plateformes transverses et services proposés

• *Systèmes d'intermédiation*

Actuellement les systèmes d'intermédiation mis en œuvre dans le SI du CNRS sont :

- un gestionnaire applicatif d'échanges et de services « outil EAI/ESB CNRS » (découpage en $\frac{1}{2}$ flux, format pivot des objets métiers échangés) qui a la responsabilité et la gestion des échanges en termes d'orchestration, de chronologie des flux le cas échéant, de transcodification des données vers les SI cibles ou depuis les SI sources ;
- un proxy de services web ;
- une exposition de services web de données de référence (mise à disposition des formats pivots persistés des objets métiers de référence)

• *Gestion des données de référence*

La DSI du CNRS dispose d'un outil GDR (Gestion des Données de Référence) nommé Réséda et proposant des services de gouvernance et de mise en qualité des données, de recherche approchant...des données de référence.

Actuellement Réséda gère les référentiels suivants (liste non exhaustive) :

- Structures organisationnelles du CNRS ;
- Personnels des structures du CNRS ;
- Fournisseurs ;
- Partenaires ;
- Contacts.

Ainsi qu'un certain nombre de nomenclatures.

La mise à disposition, au reste du SI CNRS, des données de ces référentiels se fait par les services web de données de référence (cf. plus haut).

• **Fournisseurs d'identité**

Les services d'authentification web centralisée du CNRS (web SSO) via le protocole SAML 2.0, sont regroupés sous la dénomination de Janus. Ils consistent en plusieurs fournisseurs d'identités (IdP) dépendant de la population à authentifier (Personnel des unités CNRS, Prestataires et usagers des unités CNRS, Externes) et du niveau d'authentification nécessaire.

Dans le cas où plusieurs fournisseurs d'identités peuvent être utilisés pour accéder à la solution, un mécanisme de sélection par l'utilisateur du fournisseur d'identité est mis en place. Ce mécanisme est nommé WAYF (Where Are You From).

Ils s'appuient sur le référentiel des comptes utilisateurs alimenté par le service IAM.

• **Service référentiel de comptes et gestion des accès et habilitations (IAM)**

Ce service recouvre des outils qui permettent la mise à jour du référentiel de comptes utilisateurs du SI CNRS à partir des données du référentiel des personnels des structures du CNRS.

Les données du référentiel des comptes utilisateurs sont exposées par des services Web à l'usage des applications. Elles sont également pour certaines transmises à l'application via le processus d'authentification.

Une gestion des accès applicatifs est également en place mais va évoluer dans le futur pour prendre en compte une plus grande automatisation et de nouvelles fonctionnalités pour l'attribution de rôles applicatifs à des comptes utilisateurs.

2.2.4 Prise en compte des changements de l'organisation structurelle du CNRS

Dans le cadre de la poursuite de la transformation vers un système d'information qui permet un alignement sur les stratégies de l'établissement, les outils proposés pour les SI et applications doivent prendre en considération, le plus nativement possible, les différentes restructurations du CNRS qui peuvent être classées en 2 types :

- les restructurations cycliques :
 - chaque année, une partie des unités de recherche est renumérotée, fusionnée, éclatée, ... (changement de référence métier) ;
 - les instances (conseils scientifiques du CNRS et des instituts, sections et commissions interdisciplinaires) du Comité national de la recherche scientifique (changement de périmètre sans changement systématique de référence métier) renouvelées tous les 4 ans ;
- les restructurations organisationnelles (*exemple le remplacement en 2009 des départements scientifiques par des Instituts*)

Référence	Libellé exigence	Priorité
URB_001	La solution est en capacité de fournir une continuité de service fonctionnelle dans le temps, en tenant compte des différents types de restructuration de l'organisation CNRS, impactant les SI et applications.	1

Le référentiel d'organisation du CNRS est géré via l'outil GDR, et plus particulièrement dans le référentiel Réséda Structure.

Les restructurations cycliques de l'organisation du CNRS, sont diffusées à l'ensemble du SI à partir de ce référentiel, au travers de web services.

Référence	Libellé exigence	Priorité
URB_002	La solution s'alimente du référentiel d'organisation structurelle du CNRS, à partir de ses services web dédiés.	1

2.2.5 Interopérabilité

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

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

Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Dans l'article 11 de cette ordonnance, le « RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret ».

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

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

Le titulaire respecte les dispositions du profil d'interopérabilité P1 choisi par le CNRS conformément aux objectifs du présent accord cadre.

2.3 EXIGENCES D'INTÉGRATION DANS LES SI

2.3.1 Répartition fonctionnelle

Référence	Libellé exigence	Priorité
URB_003	Pour assurer que l'architecture des solutions nationales va dans le sens d'une répartition urbanisée des fonctionnalités entre les applications selon le principe de cohérence fonctionnelle et informationnelle forte, l'équipe projet et le titulaire font valider le périmètre fonctionnel et informationnel de la solution par l'équipe urbanisation de la DSI.	1
URB_004	Lors de la conception et de la réalisation de la solution, les architectures transverses sont privilégiées, entre autres par l'utilisation des plateformes mutualisées et la réutilisation des briques applicatives (notion de service, voire micro-service). Ceci afin de ne pas implémenter ou développer une fonction ou un contrôle métier déjà outillé dans une autre application ou service.	1

2.3.2 Echanges de données

• Modalités générales

Les interfaces entrantes ou sortantes entre la solution et les autres applications du SI peuvent s'effectuer de plusieurs façons dont voici les principales : échanges de fichiers (XML, CSV, ...), échanges de messages (Broker), et services Web de type REST, tout en passant systématiquement par un des systèmes d'intermédiation du CNRS (cf. § 2.2.3).

Les échanges de données entre le gestionnaire d'échanges et de services CNRS et le site CNRS.FR ou ses sites satellites (flux entrants et flux sortants), se font au travers d'une couche d'abstraction (matérialisée par des services) pour permettre au gestionnaire d'échanges et de services CNRS d'assurer la gestion chronologique des échanges (quotidien, à la demande, ...) tout en disposant de services portés par la solution, appelables par le gestionnaire d'échanges et de services CNRS à tout moment (en journée, en traitement batch).

Au final, la solution d'échange pour chacun des flux est définie conjointement avec le CNRS dans le cadre d'ateliers de travail dans la limite des règles prévalant au CNRS sur l'intégration des SI.

Pour les flux entrants, le CNRS détermine et met à disposition, en fonction des besoins, les données échangées nécessaires au site CNRS.FR ou à ses sites satellites.

Cependant dans le cas où certains flux entrants sont à développer par le CNRS pour les besoins spécifiques de la solution, le titulaire doit déterminer son besoin au plus tôt, ajuster son planning le cas échéant, pour permettre au CNRS la mise à disposition du nouveau flux avant la livraison de la solution.

Référence	Libellé exigence	Priorité
URB_005	La solution a la responsabilité de réaliser les services d'intégration des données et les services d'exposition des informations dont elle est propriétaire. La conception de ces services est validée par le CNRS (équipes projet et transverses).	1
URB_006	Les échanges entre la solution et le reste du SI se font via des formats pivots.	1
URB_007	Les formats pivots non fournis par le CNRS sont basés sur des formats pivots existants et reconnus par la communauté. Le choix des formats pivots est validé par le CNRS (équipes projet et transverses).	1

URB_008	Les formats pivots sont facilement évolutifs en limitant les impacts sur leurs usages déjà en cours.	1
URB_009	La description des formats pivots spécifiquement développés pour le CNRS respecte un formalisme prescrit par la DSI du CNRS.	1
URB_010	La solution va chercher les objets métiers, dont elle a besoin et en récupère, au moment où elle en a besoin, uniquement la population qui l'intéresse et uniquement le sous-ensemble des caractéristiques (partie du format pivot) qui lui est nécessaire. Autrement dit, seules les données / objets métiers nécessaires sont présents dans les flux entrants de la solution.	1
URB_011	L'utilisation de données extérieures à la solution n'implique pas un stockage de ces données dans la solution, et est mis en balance avec le nombre, la fréquence et le volume des flux nécessaires pour consommer ces données, afin d'optimiser les ressources. Aussi, la nécessité de stocker les données externes dans la solution est étudiée et validée entre le titulaire et le CNRS (équipes projet et transverses).	2
URB_012	La solution expose toute la population des objets métier dont elle est maîtresse, avec le contenu complet du format pivot (FP), y compris les règles de diffusion, et/ou niveau de sensibilité. Autrement dit, la solution ne fait aucune restriction sur l'exposition des objets métier qu'elle gère.	1

• Modalités d'implémentation

Les flux d'échange de données doivent techniquement adopter les règles d'implémentation suivantes :

Référence	Libellé exigence	Priorité
ECH_001	Les échanges applicatifs avec le système d'information du CNRS s'effectuent au travers d'une solution de VPN IPSEC qualifiée ou à minima certifiés par l'ANSSI de type site à site dans une configuration conforme aux recommandations de l'ANSSI.	0
ECH_002	Les échanges inter-applicatifs passent par les systèmes d'intermédiation du CNRS. La solution ne communique qu'avec ces systèmes d'intermédiation, quel que soit le flux entrant ou sortant et propose des services permettant d'interagir avec eux.	1
ECH_003	La solution (hors progiciels) produit et reçoit des informations préformatées au format pivot défini par le CNRS. Les systèmes d'intermédiation ne portent pas les règles de gestion métier.	0
ECH_004	L'interfaçage avec les systèmes d'intermédiation est effectué via des services web du type REST. Pour la diffusion de ses données au reste du SI, la solution privilégie un appel à un service web CNRS de diffusion des données.	1
ECH_005	La fréquence des échanges de données se fait selon un mode "fil de l'eau", différentiel (plage modulable) ou complet sur validation du CNRS.	1
ECH_006	Les formats utilisés pour les échanges de données sont XML, JSON et CSV, mais ces formats ne sont pas limitatifs. Le référentiel général d'interopérabilité (http://references.modernisation.gouv.fr/interopabilite) gouverne le choix des formats.	1
ECH_007	L'encodage des données échangées est UTF-8. En cas d'impossibilité, le choix de l'encodage est étudié et validé entre le titulaire et le CNRS.	1
ECH_008	Seuls des protocoles de transport de données chiffrés sont utilisés. <i>Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés.</i>	0
ECH_009	Pour tous les types de flux transportant des données sensibles, la confidentialité des données transmises est garantie par des moyens techniques décrits dans la documentation.	0
ECH_010	Pour tous les types de flux, l'intégrité des données transmises est garantie par des moyens techniques décrits dans la documentation.	0
ECH_011	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les attaques par rejeux par des moyens techniques décrits dans la documentation.	0
ECH_012	Pour tous les types de flux, l'identité du client et du serveur de communication est garantie Par des moyens techniques décrits dans la documentation.	0
ECH_013	Pour assurer la confidentialité et l'intégrité des données lors des échanges, le chiffrement des données en supplément du chiffrement des protocoles de transport, est une mesure de protection à activer pour les données très sensibles (NIR, RIB, etc.). Ce chiffrement est réalisé à la source et le déchiffrement à la destination, sans possibilité d'interception par les systèmes d'intermédiation et de transport selon les normes de chiffrement en vigueur (cf. annexe B du RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents). Il est cependant toléré que le système d'intermédiation du CNRS assure le chiffrement en cas d'impossibilité de le réaliser à la source.	0

ECH_014	L'authentification des appels à un service web est réalisée par des mécanismes permettant de garantir la confidentialité des identifiants. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_015	Lorsque l'usage d'un broker est nécessaire, c'est celui du gestionnaire d'échange et de services du CNRS, via son API (JMS de préférence) qui est utilisé.	1

2.3.3 Authentification, comptes utilisateurs

Les services d'authentification CNRS (cf. §2.2.3) sont disponibles sur plusieurs environnements :

- production : réservé à la production de la solution,
- recette : réservé à la recette de la solution,
- formation : réservé à la formation de la solution,
- test : seul environnement accessible au titulaire, ne contenant pas de données réelles et dont l'objectif est de permettre au titulaire de valider les aspects techniques liés aux briques d'authentification.

Le titulaire assure les développements applicatifs nécessaires pour s'interfacer avec le(s) fournisseur(s) d'identité du CNRS. Si plusieurs fournisseurs peuvent être choisis, un WAYF doit être mis en place.

Le titulaire reste responsable de la solution mise en œuvre qui doit respecter les principes de fonctionnement suivants :

- L'application délègue l'authentification des utilisateurs aux services d'authentification du CNRS.
- Une fois le client SAML intégré à l'application, ce sont les fournisseurs d'identité qui se chargent d'authentifier l'utilisateur CNRS.
- L'authentification des utilisateurs par les services d'authentification CNRS est possible soit par certificats (AC CNRS / TCS), soit par email/mot de passe (en se basant sur les informations contenues dans le référentiel des comptes utilisateurs du CNRS), soit avec une solution d'authentification multi-facteurs.
- Le navigateur est toujours redirigé vers un des fournisseurs d'identité CNRS et c'est ensuite, lors de l'authentification sur ce fournisseur d'identité, que l'utilisateur peut fournir ses identifiants et authentifiants.
- Une fois l'utilisateur authentifié auprès d'un fournisseur d'identité CNRS, le navigateur de l'utilisateur envoie à l'application l'identifiant opaque dans un jeton de réponse SAML. Ce jeton contient aussi des attributs de l'utilisateur authentifié. La liste des attributs diffusés est spécifique à chaque application et limitée à ses besoins.
- Le contrôle d'accès à l'application effectué par le fournisseur d'identité CNRS se limite à dire si les informations d'authentification de l'utilisateur sont correctes. Il atteste juste que l'utilisateur est référencé dans le SI du CNRS. L'application doit assurer elle-même son contrôle d'accès à partir des rôles et droits applicatifs gérés dans l'application. Si nécessaire, les droits et profils applicatifs associés sont stockés dans la base de l'application.
- Le service provider (SP) fourni par la DSI du CNRS peut restreindre l'accès à l'application sur la base d'attributs retournés par le fournisseur d'identité.
- Le critère d'accès est donc l'appartenance ou non de l'utilisateur au référentiel des comptes utilisateurs du CNRS.
- Dans le cas d'une gestion des droits déléguée à la brique de gestion des accès et habilitations du CNRS, les rôles applicatifs peuvent être gérés et calculés de manière centralisée. Ces rôles applicatifs sont disponibles dans les services web des données des utilisateurs. Dans certains cas ils peuvent aussi être transmis à l'application lors de l'authentification. Les droits fins sont stockés et gérés dans la solution.

Référence	Libellé exigence	Priorité
AUTH_001-a	Lorsque la population utilisatrice est fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités) ou de la fédération Renater, la solution s'appuie sur ces services d'authentification pour l'authentification des utilisateurs.	1
AUTH_001-b	Lorsque la population utilisatrice n'est ni fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités), ni de la fédération Renater, les modalités de gestion des comptes permettent de garantir à tout moment : - la confidentialité des moyens d'authentification, - que seules les personnes légitimes disposent des accès. La gestion des comptes locaux lorsqu'elle est incontournable, est explicitement autorisée et documentée.	1
AUTH_002-a	Dans le cas de comptes locaux, la solution comprend des fonctionnalités de gestion de ces comptes.	0

AUTH_002-b	Dans le cas de comptes locaux, les mots de passe ne sont jamais stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible et la transformation des mots de passe fait intervenir un sel aléatoire. <i>Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les fonctions cryptographiques conformes.</i>	0
AUTH_003	Un service de découverte (WAYF) est mis en place lorsque le fournisseur d'identités CNRS n'est pas le seul fournisseur d'identité utilisé.	0
AUTH_004	La création d'un compte utilisateur pour accéder à la solution est effectuée par un mécanisme de provisioning (et non par saisie manuelle ou par création automatique sur demande de l'utilisateur directement dans la solution). Si la solution nécessite des créations de compte à l'initiative de l'utilisateur dans le cadre de téléservice, l'application de cette exigence pourra être revue après validation du CNRS. <i>Précisions : le provisioning peut être effectué via l'utilisation du service web qui expose le référentiel des comptes utilisateurs (annuaire référentiel du CNRS), à la demande ou au fil de l'eau ou via les informations issues de l'authentification.</i>	1
AUTH_005	Pour les personnels présents dans les unités du CNRS, l'origine des données pour la création et la modification des comptes utilisateurs est le référentiel des comptes utilisateurs du CNRS.	0
AUTH_006	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place (y compris pour les comptes locaux le cas échéant). <i>Précisions : la gestion du cycle de vie inclut, entre autres, des mécanismes outillés d'ajout, de suppression, et de suspension de comptes et la possibilité de gestion d'une durée de vie pour les comptes.</i>	1
AUTH_007	La modification d'un compte utilisateur dans la solution est effectuée via des services web ou via les systèmes d'intermédiation du CNRS.	1
AUTH_008	Les phases d'identification et d'authentification sont séparées de l'ensemble des actions applicatives de l'utilisateur dès la conception de la solution afin de permettre la plus grande modularité possible, et donc une facilité, quant au choix du mécanisme d'identification et d'authentification.	1
AUTH_009	Le contrôle d'accès à la solution est renforcé directement sur le reverse proxy hébergeant le Service Provider par la vérification d'un attribut spécifique exposé par le référentiel des comptes utilisateurs pour refuser l'accès aux utilisateurs authentifiés qui n'auraient pas de droits sur la solution. Dans ce cas, une page d'erreur spécifique est à prévoir pour indiquer de manière claire à l'utilisateur qu'il n'a pas les droits nécessaires pour accéder au service/à la solution. Ce contrôle s'ajoute mais ne se substitue pas aux contrôles de droits des utilisateurs réalisés par la solution.	1

Référence	Libellé exigence	Priorité
HAB_001	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs. Ces rôles applicatifs sont limités au strict nécessaire en application du principe du moindre privilège.	0
HAB_002	La solution permet de définir des rôles applicatifs en fonction des fonctions métier et du domaine d'appartenance, ainsi que des accès associés (lecture, écriture, etc.). Ces rôles sont associés à des périmètres correspondant au besoin et/ou au droit d'en connaître pour les populations considérées.	1
HAB_003	La solution permet de définir ou provisionner des comptes d'accès permanents et temporaires (définition d'une date de début et une date de fin de la validité du compte).	1
HAB_004	La solution permet la désactivation des comptes utilisateurs.	0
HAB_005	Lorsque des comptes par défaut existent, la solution permet de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur le service fourni.	1

2.4 EXIGENCES TECHNIQUES

2.4.1 Choix du CMS

La brique applicative centrale de la plateforme sera **la solution open source Drupal**. La version précise à intégrer sera déterminée au début de la phase de mise en œuvre du projet en concertation avec le CNRS.

Le choix du « thème » du backoffice sera soumis à la validation du CNRS.

Le titulaire sera force de proposition concernant l'architecture technique la plus adéquate pour répondre aux exigences du CNRS. Cette architecture sera validée en début de projet en concertation avec le CNRS.

2.4.2 Eléments techniques structurant

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

Elle est ouverte au grand public. Le Back-Office de l'application nécessite une authentification pour environ 200 contributeurs non simultanément.

En 2024, la fréquentation constatée est la suivante :

- sur le portail CNRS.FR uniquement
 - 2 701 220 visites, 1 706 236 visiteurs uniques
 - 5 890 281 pages vues, 3 463 743 pages vues uniques
 - 110 690 recherches totales, 4 586 mots-clés uniques
 - 90 531 téléchargements, 58 193 téléchargements uniques
 - 611 385 liens sortants, 394 112 liens externes uniques
 - 7400 visites par jour en moyenne
 - pic de fréquentation : 19 300 visites deux jours de suite
- sur l'ensemble des sites institutionnels (cnrs.fr, instituts, délégations)
 - 8 100 000 visites
 - 14 000 000 pages vues

2.4.3 Services d'infrastructure

• Architecture générale

La solution est construite sur une architecture logicielle intégrée, c'est-à-dire :

- s'appuyant sur une gestion des données unique,
- s'appuyant sur des mécanismes d'accès, d'authentification et de gestion de la confidentialité proposant une ergonomie homogène pour l'ensemble des fonctionnalités,
- disposant d'un outillage d'administration dédié.

Référence	Libellé exigence	Priorité
INF_001	Les privilèges accordés aux comptes de service utilisés par la solution sont limités au strict nécessaire en application du principe du moindre privilège. Les secrets associés doivent être renouvelés périodiquement. <i>Précisions : il s'agit des comptes d'accès BDD, des comptes d'accès au système de fichiers, etc.</i>	0
INF_002-a	L'administration fonctionnelle de la solution est réalisée par une IHM spécifique, si possible dédiée. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (<i>ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc.</i>).	0
INF_002-b	Des comptes d'administration dédiés (différents des comptes utilisateurs affectés aux personnels administrateurs techniques) sont les seuls utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques.	0
INF_002-c	Des moyens d'administration dédiés sont utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques. <i>Précisions : les moyens d'administration incluent les postes d'administration et leur environnement (VLAN, etc.)</i>	0
INF_003	La solution ne peut pas être proposée en mode SaaS.	0

• *Caractéristiques système*

Les exigences système suivantes doivent être respectées :

Référence	Libellé exigence	Priorité
INF_004	Le serveur HTTP de référence est Apache sur Linux. L'autre plateforme acceptée est la solution IIS sous Windows.	0
INF_005	Dans le cas où la solution nécessite un serveur d'application Java préinstallé, la référence est Tomcat. Une autre solution peut être acceptée sur dérogation.	1
INF_006	Le système d'exploitation serveur de référence est Red Hat Enterprise Linux, le système d'exploitation Windows serveur est toléré.	0
INF_007	<p>Dans le cadre de développement spécifique en PHP, la configuration d'un serveur PHP exécute uniquement les modules nécessaires à la solution, qui sont les seuls actifs. Cette liste est définie et communiquée par le titulaire.</p> <p>Certains modules sont explicitement interdits (notamment ceux permettant un appel direct au système d'exploitation).</p> <p>Certaines fonctions sont interdites : <code>disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, highlight_file, popen, proc_open, fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file, chdir, mkdir, rmdir, chmod, rename, filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo</code>.</p> <p>Pour les progiciels PHP, seules les fonctions strictement nécessaires au progiciel sont autorisées</p>	0
INF_008	Toutes les montées de versions mineures pour les OS serveurs, les modules serveurs applicatifs et bases de données, sont effectuées avec un déclenchement automatique, pour tout ce qui a été installé par le gestionnaire de paquets.	0

• *Caractéristiques réseau*

La solution mise en œuvre s'appuie impérativement sur l'infrastructure réseau existante et intègre les aspects suivants :

- tous les échanges sont compatibles avec les protocoles IPv4 et IPv6 ;
- tous les flux du système d'information sont recensés et maîtrisables, en terme de capacité à appréhender le mode de fonctionnement protocolaire associé, et à assurer le filtrage par des équipements de type « pare-feu » ; le titulaire fournit une matrice des flux de l'application, indiquant clairement les protocoles, ports et sens de communication utilisés par ces flux ;
- le serveur applicatif n'est pas directement visible des navigateurs clients, des éléments de type « reverse-proxy » étant intercalés dans le flux (Navigateur ⇄ [HTTPS] ⇒ Reverse Proxy ⇄ [HTTP] ⇒ Serveur applicatif) ;
- le fonctionnement de l'application intègre la mise en œuvre de composantes techniques souvent déployées dont notamment les réseaux privés virtuels (VLAN), la translation d'adresses IP (NAT), l'utilisation de serveurs de type Reverse Proxy, les « pare-feux », le chiffrement (via une technologie de type VPN ou autre) ;
- la solution est parfaitement inter opérante avec les principaux services Internet (DNS, SMTP, FTP, NTP, SNMP, etc.), dans leurs versions chiffrées quand elles existent. Elle respecte en particulier les principaux RFC associés à chacun des protocoles, et les règles en usage dans la communauté Internet.

Référence	Libellé exigence	Priorité
INF_009	Les flux entre les postes clients et le(s) serveur(s) applicatif(s) passent par une DMZ avec rupture de flux effectuée par exemple par des reverse proxy.	1
INF_010	<p>Les seuls flux entrant de production (hors flux techniques, <i>ex.</i> : "DNS", "EAI", ...) légitimes sont les suivants :</p> <ul style="list-style-type: none"> - reverse proxy → serveur d'application - serveur d'application → serveur de base de données 	1
INF_011	Les flux entrants de systèmes externes sont soumis à autorisation de la sécurité. Dans le cas où ils sont autorisés, ils passent par des services en DMZ.	0

INF_012	Les flux sortants initiés depuis les serveurs de la solution sont limités au strict nécessaire. Lorsque ces flux sont établis vers une zone de sensibilité moindre (<i>ex : SI usuel vers Internet, SI sensible vers SI usuel</i>), ils passent obligatoirement par des serveurs mandataires spécifiques (<i>ex : relais SMTP, DNS, NTP ou serveur mandataire HTTP</i>). Ces serveurs assurent la rupture protocolaire et contrôlent la conformité et la destination des flux. Ils sont situés dans des zones réseaux cloisonnées et dédiées à cet usage (type DMZ). Les moyens techniques utilisés sont décrits dans la documentation. <i>Précisions : cette règle est valable quelles que soient les modalités d'hébergement et les maîtres d'œuvre.</i>	1
INF_013	La compatibilité IPv6 est assurée de façon native. En production, les communications se font en IPv4 sauf décision expresse du CNRS.	2
INF_014-a	Les connexions VPN site à site sont effectuées en VPN IPSEC. <i>Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés.</i>	0
INF_014-b	Les connexions VPN client à site sont effectuées en VPN IPSEC ou VPN SSL avec authentification du terminal et de l'utilisateur.	0
INF_015	Il existe une matrice de flux bilatéraux documentée et tenue à jour pour l'ensemble des serveurs et des postes clients impliqués dans la solution. Cette matrice de flux est techniquement implémentée sur des dispositifs de filtrage (pares-feux). Les flux non explicitement déclarés dans la matrice de flux sont techniquement interdits.	0
INF_016	L'administration technique de la solution passe par un bastion d'administration assurant la traçabilité des actions.	0
INF_017	La prise de main à distance d'un actif quelconque de la solution (serveur, actif réseau, poste de travail...) depuis l'extérieur passe par un VPN puis un bastion.	0

• **Exploitabilité de la solution**

L'application doit être techniquement paramétrable à souhait, et elle doit être facilement exploitable par les équipes qui la maintiennent en condition opérationnelle. En particulier, les exigences suivantes sont à respecter par l'application :

Référence	Libellé exigence	Priorité
INF_018	L'infrastructure gère la résilience applicative à son niveau en redémarrant automatiquement les machines virtuelles dont le serveur deviendrait indisponible. Lorsque le métier exprime des besoins de disponibilité ou de capacité supérieurs l'application est capable de fonctionner avec plusieurs instances applicatives actives, en utilisant toujours une seule instance de base de données.	0
INF_019-a	Les sauvegardes sont déportées pour être suffisamment isolées du site de production.	0
INF_019-b	Les sauvegardes font l'objet de dispositions de protection physiques et logiques permettant d'assurer le même niveau de disponibilité, de confidentialité et d'intégrité que l'environnement de production.	0
INF_020	Les technologies à base de containers (de type Docker) ne sont pas préconisées tant que le CNRS ne s'est pas doté de l'outillage adapté.	1
INF_021	L'application est compatible avec un environnement d'exécution durci selon les règles définies par le CNRS, ces règles sont issues des profils SCAP d'une version 1.3 ou supérieure publiés par le NIST pour les systèmes d'exploitation.	1

2.4.4 Architecture applicative

Ces exigences s'appliquent uniquement sur les développements logiciels spécifiques réalisés dans le cadre de ce marché. Ils ne s'appliquent pas à la plateforme Drupal.

• **Normes d'architecture**

Les exigences et recommandations techniques concernant l'architecture applicative sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_001	L'architecture sépare bien les aspects essentiels de la solution (présentation, aspects métiers, accès aux données) afin de faciliter la testabilité et l'extensibilité de la solution. Une attention particulière est portée à l'abstraction de la base de données, afin de permettre la mise en place de l'intégration continue du code et faciliter les éventuels changements de base de données.	0
DEV_002	Les mécanismes de redondance et de haute disponibilité sont mis en œuvre sur les ressources de la solution le nécessitant pour répondre au besoin de disponibilité et de continuité de service de la solution.	0
DEV_003	L'architecture est de type client léger, les clients lourds ou riches basés sur des technologies de plugins dans les navigateurs (tels que les applets, Flash, ActiveX, ...) sont interdits. Tous les traitements et vérifications sont réalisés au moins du côté serveur : aucune entrée cliente n'est considérée comme fiable par défaut.	0
DEV_004	L'usage de Java WebStart est interdit.	1
DEV_005	Il est interdit de déployer sur les postes de travail des logiciels créant des adhérences autres que le navigateur, en dehors de certaines exceptions à justifier.	1
DEV_006	La solution est utilisable à partir d'un navigateur Web sur un protocole de transport TLS aussi bien pour les solutions à visibilité internet que les solutions internes.	1
DEV_007	Le CNRS impose les technologies Web natives (HTML5, CSS3...) limitant les interactions avec le système d'exploitation et le respect des standards du W3C.	1
DEV_008	En plus du français, la gestion d'au moins une langue étrangère (l'anglais) est fournie.	1
DEV_009	Les libellés (messages d'erreur, champs, texte, ...) sont externalisés, soit en base soit via un fichier de propriétés. <i>Par exemple, les nomenclatures ne sont pas stockées dans le code applicatif mais sont externalisées.</i>	1
DEV_010-a	Toute émission de mails doit respecter les règles suivantes : 1. L'expéditeur (« from » de l'entête ET de l'enveloppe) utilise un sous-domaine de cnrs.fr dédié à l'application (<i>ex : @monappli.cnrs.fr</i>). 2. L'application utilise le relai SMTP local du serveur pour l'envoi des mails, soit de manière implicite, soit en spécifiant l'usage du relai localhost « 127.0.0.1:25 » si nécessaire. Ce relai local acheminera alors les mails vers les relais centralisés qui assureront l'émission externe, en cohérence avec le SPF du domaine d'émission. 3. Le domaine de sortie est choisi parmi ceux autorisés par les relais de la DSI. 4. La solution n'utilise pas l'adresse mail des utilisateurs pour les domaines non gérés par la DSI comme clause FROM, sous peine d'usurpation d'identité et blacklistage (par exemple, il est interdit d'envoyer des mails de type john.doe@google.com).	0
DEV_010-b	1. La solution supporte l'envoi de messages numériquement signés par le standard S/MIME 2. Il est recommandé de ne pas envoyer de pièces jointes, dans le cas où ce serait nécessaire, la solution permet le paramétrage de la limite de taille des pièces jointes. 3. La solution prévoit des envois par lots en cas de besoin, et limite le nombre de destinataires par lot et la fréquence d'envoi. En cas de besoin d'envoi de messages aux utilisateurs de la solution, un serveur SMTP dédié (fourni par la DSI) est utilisé.	1
DEV_010-c	L'émission de messages de type email par la solution est contrôlée afin d'éviter le détournement de la fonction (spam ou diffusion de contenu malveillant) : - L'émetteur est fixé de façon fiable sur une adresse et un nom d'expédition n'autorisant pas de réponse (« noreply@monappli.cnrs.fr ») et identifiant clairement l'application émettrice. - La liste des destinataires est également maîtrisée dans les paramètres de l'application (<i>ex : listes préétablies ou listes de diffusion, domaines cibles en liste blanche, nombre de destinataires limités, etc.</i>). - Le contenu des messages repose sur des modèles préétablis et n'incluant pas de code pouvant être interprété de façon détournée par les clients. A ce titre, l'envoi de messages au format « texte brut » et sans pièce jointe est à privilégier.	0

• *Langages*

Les exigences et recommandations techniques concernant les langages utilisés sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_011	Dans le cadre de développement spécifique, l'ensemble des langages et des composants nécessaires à la solution sont utilisés dans les versions mentionnées dans le document : CNRS.fr_CCTP-Livret1_Annexe_CCT_Versions_cibles (ce document est mis à jour régulièrement). Le document, dans sa version courante est applicable à tout moment, ce qui implique des mises à jour régulières des applicatifs en conséquence.	0
DEV_012	Sauf contrainte contractuelle, le choix du langage et des frameworks est le résultat d'un consensus entre la DSI et le titulaire en charge de la réalisation de la solution.	0
DEV_013	Les frameworks de développement sont ouverts, éprouvés, avec une large communauté active, maîtrisés par le titulaire en charge de la réalisation de la solution, et permettent d'automatiser les tests unitaires. Leur choix est justifié en regard des gains attendus en termes de développement et d'évolutivité. Les versions utilisées sont systématiquement celles qui sont les plus récentes et qui présentent la durée de support la plus longue.	1
DEV_014	Pour une solution Java, le framework utilisé est Spring Boot avec le serveur web embarqué (la solution ne requiert donc pas d'être installée dans un conteneur de servlets).	1
DEV_015	Pour une solution PHP, le framework utilisé est Symfony.	1
DEV_016	Le nombre de composants externes complémentaires est limité au strict minimum. L'utilisation de composants externes, progiciels, logiciels tiers respecte les règles suivantes : 1. Son fournisseur est engagé sur le maintien dans la durée d'une réelle API de communication 2. Les évolutions de la solution peuvent être menées sans avoir systématiquement recours à des consultants experts de ces composants tiers. 3. Les développements spécifiques n'ont pas d'impact sur les montées de version, ou bien ces impacts sont intégrés comme un coût additionnel en début de projet 4. Le code tiers utilisé dispose d'une licence d'utilisation bien identifiée, n'induisant pas pour le CNRS de contraintes d'acquisition ou d'aliénation de ses droits. Les licences libres sont recommandées.	0

• *Normes de développement*

En fonction de la technologie retenue, des préconisations concernant les méthodologies et règles de développement sont applicables et s'appliquent notamment pour le code spécifique développé pour le CNRS.

Les recommandations ci-après s'appliquent de manière plus générale à l'ensemble des technologies.

Le CNRS est attentif à la qualité logicielle de l'application et à ses capacités d'évolution.

D'une manière générale, le titulaire doit utiliser autant que possible des standards pérennes normalisés ou reconnus du marché.

Les exigences et recommandations techniques concernant les normes de développement sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_017	Les développements sont modulaires afin de faciliter la maintenance et l'évolutivité du code.	0
DEV_018	Les erreurs sont traitées de manière à assurer la sécurité dans les développements (toutes les erreurs levées lors de l'exécution sont traitées en conséquence).	0
DEV_019	Les bibliothèques de logs utilisées sont ouvertes, éprouvées, avec une large communauté active, et maîtrisées par le titulaire. Les logs sont paramétrables et gèrent a minima les niveaux suivants : - ERROR : une erreur technique non récupérable est survenue dans la solution ; en général, la solution n'est plus opérationnelle ensuite - WARN : un point d'attention a été soulevé, ou une erreur récupérable est survenue - INFO : permet de suivre le fonctionnement métier de l'application, plus les étapes importantes de la vie de l'application - DEBUG : permet de voir le fonctionnement technique de la solution.	0

DEV_020-a	La solution journalise des événements permettant l'audit des connexions effectuées à la solution, et le suivi des opérations importantes.	0
DEV_020-b	Dans le cadre de développement spécifique, l'application utilise une librairie de logs qui permet de paramétrer la destination des événements de logs (par exemple syslog).	0
DEV_021	Les opérations à tracer ainsi que le format du contenu de ces journaux sont définis conjointement entre le titulaire et le CNRS, les logs issus de l'application sont dans des fichiers textes dans un format permettant leur analyse.	0
DEV_022	Dans le cadre de développement spécifique, la solution ne récupère pas de code externe (en dehors de sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.	0
DEV_023	Dans le cadre de développement spécifique, le paramétrage technique de la solution est réalisé au travers de fichiers de configurations qui sont stockés de manière indépendante du code applicatif.	0
DEV_024	La solution met en œuvre des mécanismes de protection contre les différents types d'injection (liste non exhaustive : SQL, shell, Ldap,...)	0
DEV_025	Dans le cadre de développement spécifique, les tests unitaires sont automatisés, avec un taux de couverture minimum défini d'un commun accord entre tous les acteurs du projet. Ces tests s'exécutent sans erreur dans la forge du CNRS (les cas d'erreurs résiduels seront justifiés par le titulaire).	0
DEV_026	Des frameworks sont utilisés pour développer les tests unitaires, dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Les tests unitaires livrés en même temps que les fonctionnalités couvertes servent aux tests de non régression et peuvent fournir à travers des outils de couverture de tests un indicateur de qualité.	1
DEV_027	Dans le cadre de développement spécifique, les codes sont documentés et lisibles. Les composants (modules, classes, méthodes) reposent sur une nomenclature de nommage normalisée et cohérente.	0
DEV_028	Dans le cadre de développement spécifique, pour les langages supportant les packages ou modules, les éléments de code source doivent être organisés avec le préfixe « fr.cnrs »	0
DEV_029	Au niveau OS, le jeu de caractères pour la solution est UTF-8.	1
DEV_030	<p>Les solutions sont compatibles avec la liste des navigateurs/OS et versions associées dans le document CCT-Versions-cibles (ce document est mis à jour régulièrement).</p> <p>La notion de support d'une plate-forme cliente impose que l'ensemble des fonctionnalités attendues soit disponible dans des conditions de complétude, d'ergonomie et de performance tout à fait normales.</p> <p>Les niveaux de prises en charge possibles sont les suivants :</p> <ul style="list-style-type: none"> - Maximal : Les navigateurs dans cette catégorie offrent aux visiteurs toutes les performances techniques, visuelles et fonctionnelles définies par le cahier des charges et la maquette graphique, - Dégradé : Les navigateurs permettent une expérience utilisateur équivalente au niveau précédent mais qui peut toutefois présenter des différences considérées comme négligeables (décalages minimes, arrondis, ombrages...), - Minimal : L'intégration HTML/CSS est accessible et agencée convenablement, mais aucun effort n'est porté sur la compatibilité visuelle avec les niveaux précédents. 	0
DEV_031	Dans le cadre de développement spécifique, l'utilisation de Javascript est autorisée notamment pour fluidifier les échanges avec la solution, <i>par exemple en effectuant des contrôles côté client</i> . Cependant, ces contrôles côté client ne se substituent pas aux contrôles côté serveur qu'il faut impérativement réaliser.	0
DEV_032	Dans le cadre de développement spécifique, il est interdit de construire un framework Javascript.	0
DEV_033	L'architecture de services web recommandée est l'architecture de type REST.	1
DEV_034	Dans le cadre de développement spécifique, l'outil de génération de PDF est opensource, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_035	Les outils de requêtage mis à disposition sont paramétrés de manière à limiter les risques de dégradation des performances de la plate-forme en cas d'utilisation malavisée par certains utilisateurs. Les outils de requêtage garantissent le respect des droits d'accès de l'utilisateur.	0
DEV_036	Les éléments d'architecture critiques, complexes ou difficiles à appréhender font l'objet de paragraphes spécifiques dans la documentation permettant leur bonne compréhension.	0

DEV_037	Les dossiers d'architecture technique, spécifications techniques détaillées (STD) ainsi que les manuels d'exploitation (MEX) et d'installation (MINS) sont actualisés par le titulaire autant que de besoin. Ils sont réputés être à jour à tout moment.	0
DEV_038	La gestion des types d'environnements (développement, recette, production, ...) est prise en charge dans la solution pour adapter automatiquement le niveau de fonctionnalité de la solution (<i>exemple : activation du debug, paramétrages d'envoi de mails, etc.</i>). Les propriétés de l'environnement sont renseignées sur l'instance déployée et facilement modifiables (<i>exemple : fichier unique à modifier au moment du déploiement</i>)	2
DEV_039	L'ensemble des éléments du bandeau, l'ensemble des couleurs, des polices de caractères, des espaces, filets, comportements au passage de la souris, aplats couleurs, paramétrages de tableaux, gestion des menus et onglets, sont gérés par une feuille de style CSS (pas de code couleur ni de mise en page en dur dans le code de la page).	1
DEV_040	Le développement (code et organisation de page) est conçu en accord avec les règles d'accessibilité du RGAA.	0
DEV_041	Éviter au maximum l'utilisation de tables pour gérer la mise en forme dans le code HTML.	2
DEV_042	Les configurations des middlewares et des logiciels embarqués dans la solution sont durcies. <i>Précisions : les guides de durcissement des éditeurs et constructeurs et les guides de durcissement de l'ANSSI sont à appliquer.</i>	0

• *Outillage de développement*

Le CNRS opère une forge logicielle afin de favoriser la qualité logicielle, la réduction de la dette technique et l'intégration continue.

Cette forge est composée des éléments suivants :

- un service de gestion de configuration et de dépôt interne : Gitlab
- un service d'intégration continue : Gitlab CI et Gitlab runners
- un analyseur de code : Sonar
- un gestionnaire d'artéfacts : Artifactory

Le CNRS encourage toute initiative du titulaire pour utiliser un outil d'analyse et de mesure d'écoresponsabilité du code produit, et fournir des indicateurs associés.

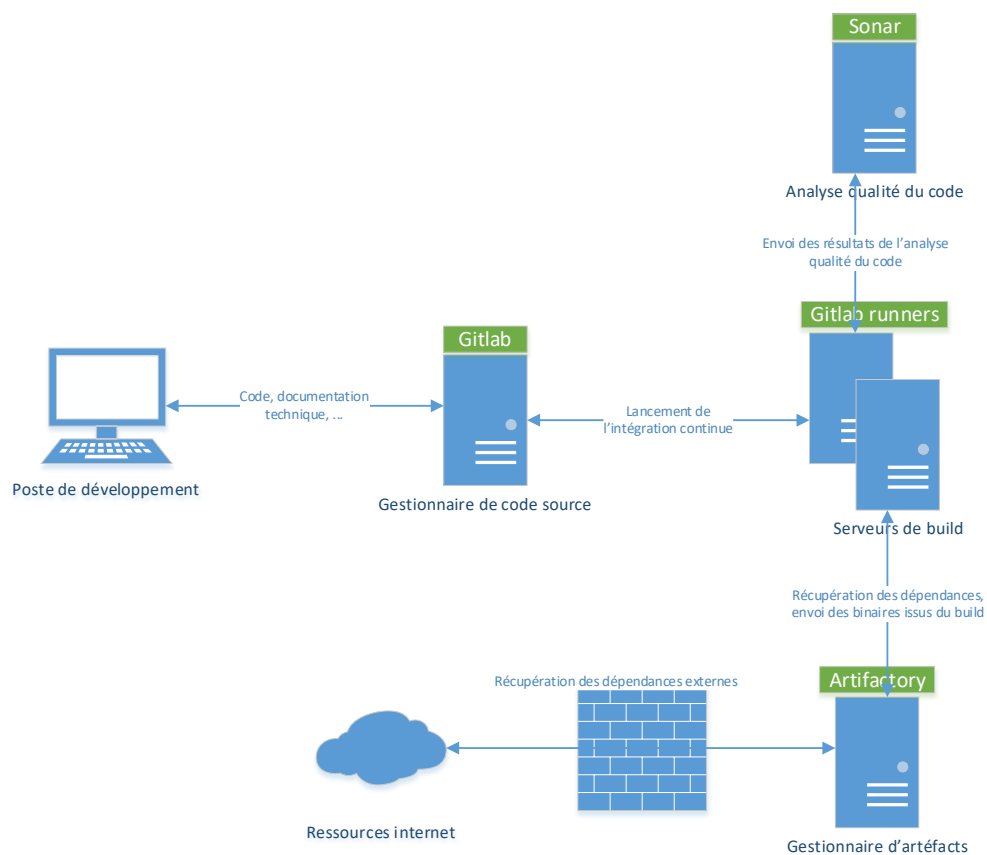


Figure 1 : Présentation de la forge logicielle



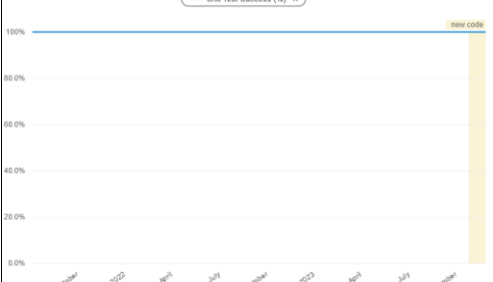
Le CNRS utilise les outils Ansible et Tower pour automatiser autant que possible le déploiement de ses applications.

L'outil de vérification de la qualité du code utilisé à la DSI est SonarQube (<https://www.sonarsource.com/products/sonarqube/>).

Au démarrage de l'accord-cadre, les équipes CNRS et titulaire se mettent d'accord sur le profil SonarQube à utiliser afin d'évaluer la qualité du code source.

Les métriques particulièrement suivies par le CNRS sont les suivantes :

Métrique SonarQube	Description métrique	Cible CNRS
	Taux de commentaires	<i>Le seuil sera défini au lancement du projet</i>
	Duplication de code	<i>Le seuil sera défini au lancement du projet</i>

Métrique SonarQube	Description métrique	Cible CNRS
	Respect des règles de codage, problèmes potentiels de sécurité	Pas d'anomalies de niveau « blocker » et « critical ». Analyser les majeures. Pas de vulnérabilités.
	La couverture de tests unitaires (pourcentage de lignes de code du projet qui est appelé pendant la phase de test)	Supérieur à 50%
	Le taux de succès des tests unitaires	égal à 100%

Le niveau de conformité à atteindre fait l'objet d'une concertation entre le titulaire et le CNRS.

Plus que l'atteinte de seuils définis, le CNRS est attentif à l'évolution des métriques au cours du temps (lors de chaque livraison majeure de l'application).

Les exigences concernant les outils de développement du titulaire sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_043	Le titulaire choisit l'outil de développement intégré (IDE) dont il a la maîtrise. Celui-ci est maintenu.	2
DEV_044	Dans le cadre de développement spécifique, pour les cas qui nécessitent des interactions avec des éléments externes (tests, environnement d'intégration ou de recette, ...), des mocks/bouchons sont utilisés. L'usage de bibliothèques de mocks est possible. Le CNRS n'impose pas d'outil particulier dans la mesure où celui choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_045	JMeter est l'outil préconisé pour les tests de charge, si un autre outil est proposé il est ouvert, éprouvé, avec une large communauté active, et maîtrisé par l'équipe en charge de son utilisation.	1
DEV_046	Un moteur de production est utilisé afin de gérer les dépendances de la solution, le lancement des tests automatisés, sa construction, la publication des artefacts sur un gestionnaire d'artefacts, ... Pour les projets Java, Maven ou Gradle est utilisé. Pour les projets PHP sous Symfony, Composer est utilisé.	1
DEV_047	Le nommage des artefacts générés par la phase de construction de la solution suit les normes de nommage standard (<i>par exemple Maven pour les projets Java, Composer pour les projets PHP</i>).	1
DEV_048	Dans le cadre de développement spécifique, le gestionnaire de source Git est utilisé pour la gestion des codes sources. Le CNRS dispose d'un outil de gestion de code source dans lequel se trouve le code source de la solution (soit en posant les commits directement dans le dépôt Git du CNRS, soit avec un mécanisme de synchronisation - à la charge du titulaire - dans le cas où le titulaire souhaite utiliser des dépôts Git qui ne sont pas ceux du CNRS).	0
DEV_049	Dans le cadre de développement spécifique, la notion de tag (au sens Git) est utilisée pour faire le lien entre les modifications de code source et la version de la livraison.	0
DEV_050	Un modèle de gestion des branches Git est utilisé (<i>par exemple Gitflow</i>) en accord avec le CNRS.	1

DEV_051	Le CNRS dispose d'un outil d'analyse statique de code source, utilisé pour analyser le code de la solution. Le titulaire a la possibilité d'utiliser également un outil d'analyse de qualité du code, qui peut ne pas être celui du CNRS. Des indicateurs et des métriques de qualité logicielle reposant sur ces outils sont proposés par le titulaire. Les éléments de qualité remontés par l'outil d'analyse statique du code du CNRS et analysés ensuite, sont définis au démarrage du projet.	1
DEV_052	Le CNRS dispose d'un outil d'intégration continue, utilisé a minima pour lancer l'analyse via l'outil d'analyse statique du code. De manière générale, la solution est construite par cet outil d'intégration continue. Le code source contient un fichier indiquant la marche à suivre pour construire le projet (ce qui inclut au minimum la récupération des dépendances, le lancement des tests automatisés, la construction de la solution et la publication des artefacts). Tout autre mode de construction est à discuter au démarrage du projet.	1
DEV_053	Le titulaire exécute une tâche de construction automatique avant toute livraison au CNRS afin de valider la bonne réalisation des opérations de compilation, de réussite des tests unitaires ainsi que de vérifications des éventuelles licences.	1
DEV_054	La livraison et l'installation de la solution est réalisée de façon outillée et automatisée en évitant toute opération manuelle (sauvegarde système, actions en base de données, mise à jour de fichiers, ...). L'application est conçue de telle manière que sa livraison et son installation sont réalisables avec l'outil d'orchestration du CNRS. Le cas échéant, l'outillage écrit pour réaliser cette tâche est également géré dans l'outil de gestion de code du CNRS.	1
DEV_055	Dans le cadre de développement spécifique, le titulaire se synchronise avec le gestionnaire de version (Git) du CNRS à chaque livraison pour le code spécifique développé pour le CNRS afin que le CNRS ait une visibilité sur le code, les tests unitaires et les tests d'intégration associés.	0
DEV_056	La réussite de l'ensemble des tests unitaires est une condition nécessaire à l'acceptation d'une livraison majeure. Le niveau de réussite des tests unitaires à atteindre peut cependant faire l'objet d'une concertation en cas de forte contrainte au cas par cas.	1
DEV_057	Les modifications de schémas de base de données sont automatisées par l'application soit par le lancement de commandes de migration fournies par le framework, soit lors du démarrage de l'application.	1

2.4.5 Base de données

Les exigences et recommandations techniques concernant les bases de données sont les suivantes :

Référence	Libellé exigence	Priorité
BDD_001	Dans le cadre de développement spécifique, une base de données (relationnelle ou non relationnelle si c'est pertinent) est utilisée pour gérer la persistance des données.	0
BDD_002	Les solutions de SGBD de référence sont PostGreSQL et MongoDB.	1
BDD_003	La non adhérence au SGBD est assurée, les requêtes ne sont pas implémentées directement dans le code applicatif (batchs compris), ni au travers de procédures stockées. Dans le cas des langages orientés objet, un ORM (mapping entre le modèle relationnel et le modèle objet) est utilisé. Dans les autres cas, une couche d'abstraction de la base de données est utilisée. Lorsque des requêtes SQL sont implémentées, elles le sont en respectant le standard SQL ANSI.	1
BDD_004	Au niveau SGBD, le jeu de caractères utilisé est UTF-8	1
BDD_005	Tous les objets de la base de données sont documentés.	1

2.4.6 Engagements de qualité de service pour l'application

• *Disponibilité*

Dans le cas d'une phase de migration en production (portage), une interruption de service de 2 jours maximum est envisageable.

Dans le cas d'un déploiement d'une nouvelle version (mise en production) ou en cas de maintenance programmée, l'interruption de service acceptable est de 1h en continu une fois par mois.

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

Il est à noter qu'étant donné le caractère particulier d'une application fonctionnant selon un calendrier événementiel, l'application reste disponible et performante, en particulier pendant les pics d'utilisation de fin de période.

● *Intégrité*

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

En cas de corruption de données, la base doit pouvoir être restaurée juste avant la corruption. Si nécessaire, l'application doit avoir la possibilité de reprendre les flux ou les batch qui auront été générés lors de la période où la base était corrompue.

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

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

● *Performances*

Le temps d'affichage d'une ressource (page, requête de recherche, etc.) doit être inférieur ou égal à 1 seconde.

Ce temps de réponse est mesuré sur un échantillonnage défini conjointement avec le CNRS au démarrage du projet, à partir d'un poste de supervision hébergé sur le même réseau en amont du reverse proxy.

Si des cas particuliers dérogent à cette règle, ils doivent faire l'objet d'un accord explicite du chef de projet DSI.

Le titulaire fournit au CNRS :

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

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

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

La solution applicative devra respecter les critères et les niveaux de performance suivants :

La solution sera conçue prioritairement pour mobile, et déclinée, optimisée pour tous les autres terminaux. Seront pris en compte les périphériques mobiles, jusqu'aux grands écrans 4K.

Le titulaire s'alignera sur les critères de performance et de bonnes pratiques conformes à l'état de l'art, en s'aidant d'outils de type PageSpeed Insights ou Lighthouse. Une attention particulière sera portée sur les signaux vitaux (mobile et bureau) et aux statistiques. Les scores seront majoritairement au-dessus de 90%, et aucun score sous le seuil des 49%.

Le titulaire s'alignera également sur les critères et bonnes pratiques recommandées par Green IT. Les mesures peuvent être prises par l'outil Green-IT CLI par exemple, pour produire les rapports. Des rapports sur certains parcours pourront être générés, une fois les parcours de navigation définis avec le CNRS. Ces rapports prennent également en compte, de manière non exhaustive, la présence de ressources en cache, la compression et la minification, l'utilisation du http/2, la présence d'image retaillées dans le navigateur, etc.

Le suivi, autant que possible, de ces critères, doit garantir au moins en partie la qualité de l'expérience utilisateur, de la performance et d'un moindre impact environnemental.

Le titulaire sera force de proposition dans les solutions mises en place.

Le CNRS attend néanmoins :

- Gestion du cache (pages, blocs, vues, entités)
- Selon l'architecture choisie, gestion de cluster Redis, Memcached, OPcache et APCu
- Optimisation du code et des bases de données
- Agrégation des fichiers
- Minification du CSS et JS

- Compression des données transmises
- Utilisation de CDN, en respectant les exigences de sécurité du CNRS
- Optimisation des images (compression, formats webp et avif, lazy loading)
- Usage préférentiel du CSS pour les éléments interactifs et animés
- Réduire le nombre de modules au minimum, en veillant à ce qu'ils soient maintenus par la communauté, reconnus par la Security Team de Drupal dans la mesure du possible. Les modules inutilisés devront être supprimés.

2.5 EXIGENCES DE SÉCURITÉ

Les exigences et recommandations de sécurité sont les suivantes :

Référence	Libellé exigence	Priorité
SEC_004	<p>Le titulaire intègre dans sa proposition d'architecture une infrastructure conforme aux guides de l'ANSSI, en particulier :</p> <ul style="list-style-type: none"> - Recommandations relatives à l'interconnexion d'un SI à Internet (https://cyber.gouv.fr/publications/recommandations-relatives-linterconnexion-dun-si-internet), sur la construction d'un SI web connecté à internet (Pare-feux, DMZ, WAF, etc.) - Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet (https://cyber.gouv.fr/publications/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-internet) - Recommandations de sécurité pour l'architecture d'un système de journalisation (https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation)https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation) - Recommandations relatives à l'administration sécurisée des SI (https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si) 	0
SEC_005	Le titulaire protège l'infrastructure à l'aide d'une solution d'EDR souveraine exploitée par une équipe qui répond aux exigences de protection des données à caractères personnelles qui s'appliquent au CNRS.	0
SEC_006	Le titulaire met en place une connexion aux Back-Office de l'écosystème à travers une connexion VPN client avec une authentification renforcée (cf. 1.6.1 Authentification et comptes des utilisateurs)	0
SEC_007	Le titulaire met en œuvre un Back-Office séparé du Front-Office par un système de segmentation réseau et des serveurs dédiés.	0
SEC_008	<p>Le titulaire met en œuvre :</p> <ul style="list-style-type: none"> - un Web Application Firewall (WAF en mode « whitelist ») afin de protéger les contenus publiés par le Front-Office, - un ou plusieurs dispositifs anti-DDoS - et un dispositif de lutte contre les robots et les automatisations malveillantes. <p>Le titulaire est en charge de la configuration, l'exploitation et les recettes de ces outils.</p>	0
SEC_009	Le titulaire met en place un dispositif qui protège les contenus publiés par le Front-Office contre toutes les modifications abusives, avec un système de détection et de réaction automatiques en cas d'anomalie de publication (mise hors ligne, republication antérieure, etc.).	0

2.6 EXIGENCES D'ERGONOMIE-GRAPHISME

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

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

Les éléments concernant l'ergonomie et le graphisme pourront être ajustés en cours de réalisation, de manière concertée entre le titulaire et l'équipe projet CNRS.

2.6.1 Charte graphique

Le titulaire s'appuiera sur le design system du CNRS, il couvre les questions d'accessibilité numérique et les bonnes pratiques. Néanmoins, la manière dont il sera exploité et mis à jour, doit respecter l'ensemble des critères décrits ci-dessous (liste non exhaustive), ainsi que la réglementation (RGAA, RGESN).

Référence	Libellé exigence	Priorité
ERG_001	L'interface de la solution respecte la charte du CNRS. Les éléments de base sont décrits dans le design system du CNRS (couleurs, comportements, titraillies, boutons, navigation...), sous la forme d'un guide et d'un kit UI, conçus sur Figma. Un accès « dev mode » pourra être mis à disposition du futur titulaire.	1
ERG_002	L'ensemble de la solution utilise les mêmes éléments de la feuille de style de manière logique et uniforme : police de caractère, liens de navigation, intitulés de champ, titres de différents niveaux, messages informatifs et d'aides à la saisie, messages d'alerte, etc. Il en est de même pour la sémiologie des pictogrammes.	0
ERG_003	Solution responsive, l'organisation des écrans s'appuie sur des grilles (grid). Toutes les fonctionnalités essentielles de la solution sont accessibles quel que soit le média, et respecte une égalité de traitement dans l'accès à l'information (accessibilité numérique). L'ensemble des interfaces sont conçus en <i>mobile first</i> , puis déclinés et optimisés pour les autres terminaux.	1

Le titulaire respectera les règles OPQUAST suivantes :

Numéro	Règle Opquast ²
175	La charte graphique est cohérente sur l'ensemble du site.
176	L'information n'est pas véhiculée uniquement par la couleur. Fournir un complément à la couleur pour véhiculer l'information qu'elle porte.
177	Les contenus sont présentés avec un contraste suffisant par rapport à leur arrière-plan. Veiller à conserver un ratio de contraste minimal de 3:1 entre le texte et son arrière-plan, tel qu'il peut être mesuré via l'algorithme WCAG2.0.
178	Le contenu et le sens de chaque page ne sont pas altérés lorsque les styles sont désactivés.
180	Un contenu qui doit être restitué dans un lecteur d'écran ne lui est pas dissimulé. Par exemple à travers la propriété display ou visibility.
181	La taille des éléments cliquables est suffisante.
182	Les textes pouvant être mis en forme via des styles ne sont pas remplacés par des images.
183	Les contenus générés via les styles sont dotés d'une alternative appropriée.
184	Les pictogrammes typographiques sont dotés d'une alternative appropriée.
185	Une famille générique de police est indiquée comme dernier élément de substitution. Dans le cas du CNRS, il s'agit de la police « Arial », sans serif.
187	Les mises en majuscules à des fins décoratives sont effectuées à l'aide des styles
188	Le site ne bloque pas les fonctionnalités de zoom du navigateur. Par exemple ne pas utiliser les attributs minimum-scale, maximum-scale et user-scalable de l'élément meta viewport.
189	Le site propose un ou plusieurs mécanismes dédiés à l'adaptation aux terminaux mobiles. Le CNRS demande une conception mobile first.
190	Le site propose des styles dédiés à l'impression.
191	Le contenu de chaque page est disponible à l'impression sans blocs de navigation.

² <https://checklists.opquast.com/fr/assurance-qualite-web/>

2.6.2 UX/UI et règles d'ergonomie

La solution est ergonomique c'est-à-dire qu'elle est facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale. Le temps d'apprentissage pour les usagers, externes ou contributeurs, doit être réduit au minimum.

La solution accompagne l'utilisateur qui sait ce qu'il doit faire sur la page active. Il peut également pouvoir naviguer et se repérer dans l'ensemble des interfaces. Pour cela, la solution utilise les systèmes de navigation les plus adaptés, *par exemple : menus, onglets, enchaînements d'étapes, etc.* décrits dans les CCTP et le design system CNRS.

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

La conception de l'interface fera appel à des composants innovants et des micro-interactions, *par exemple : effets de transition, barre de progression, auto complétion et suggestion, etc.* en restant vigilant sur les exigences d'accessibilité numérique et de performance. Entre plusieurs composants rendant le même service, le choix sera guidé par des critères d'écoresponsabilité (poids du composant, consommation en ressources, pérennité et maintenabilité).

L'application est conçue de manière globale et homogène.

Référence	Libellé exigence	Priorité
ERG_004	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal, sauf fonctionnalité particulière demandée par le CNRS	1
ERG_005	Les tableaux sont conçus de manière optimisée (utilisation de formules synthétiques, de pictogrammes, interlignages valorisés par des couleurs de fond, mise en valeur des entêtes, des liens, ordre des colonnes pertinent, système de navigation pour les tableaux longs).	1
ERG_006	Les titraillies et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).	0
ERG_007	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.	1
ERG_008	Solution responsive, l'interface est adaptée au pilotage de l'interface via un doigt (zone cliquable agrandie, survol impossible, navigation par balayage de l'écran, etc.).	1

Les règles ci-dessous, s'ajoutent au design system CNRS. Chacune de ces lignes doit venir le compléter et le titulaire doit s'assurer de leur bonne application. Le titulaire trouvera l'ensemble des [critères Opquast en ligne](#).

Numéro	Règle Opquast ³
149	La navigation sur le site ne provoque pas l'ouverture de popups. Préférer l'usage de « popins », et avec parcimonie.
150	Il est possible de revenir à la page d'accueil depuis toutes les pages.
152	Les items actifs de menu sont signalés.
154	Les icônes de navigation sont accompagnées d'une légende explicite (Ex : alternative textuelle, balisage ARIA)
155	Les mécanismes de fermeture de fenêtres sont visuellement rattachées à leur contenu.
157	Les nouvelles fenêtres dimensionnées et les fenêtres modales sont dotées d'un bouton de fermeture explicite.
159	Chaque page contient des liens d'accès rapide placés au début du code source.
160	Le focus clavier n'est ni supprimé ni masqué.
161	Le site est intégralement utilisable au clavier.
162	La navigation au clavier s'effectue dans un ordre prévisible.
69	L'étiquette de chaque champ de formulaire indique si la saisie est obligatoire.
70	Le format de saisie des champs de formulaire qui le nécessitent est indiqué
75	Chaque étiquette de formulaire est visuellement rattachée au champ qu'elle décrit.
77	En cas de rejet des données saisies dans un formulaire, les champs contenant les données rejetées sont indiqués à l'utilisateur.
78	En cas de rejet des données saisies dans un formulaire, les raisons du rejet sont indiquées à l'utilisateur.

³ <https://checklists.opquast.com/fr/assurance-qualite-web/>

81	Lors de la saisie d'un formulaire réparti sur plusieurs pages, un récapitulatif global est affiché avant l'envoi définitif.
83	La soumission d'un formulaire est suivie d'un message indiquant la réussite ou non de l'action souhaitée.
84	L'utilisateur est averti au début d'un processus complexe de la nature des données et documents exigés.
85	Les processus complexes sont accompagnés de la liste de leurs étapes.
86	L'étape en cours d'un processus complexe est indiquée.
121	Les animations, sons et clignotements peuvent être mis en pause.
133	Les liens de même nature ont des couleurs, des formes et des comportements identiques sur toutes les pages.
134	Le soulignement est réservé aux liens.
135	Les liens sont visuellement différenciés du reste du contenu.
150	Il est possible de revenir à la page d'accueil depuis toutes les pages.
216	Le serveur envoie une page d'erreur 404 personnalisée.
217	Le serveur envoie une page d'interdiction 403 personnalisée.
218	Le menu principal de navigation figure sur les pages d'erreur personnalisées.

3 POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION (PSSI)

Le CNRS met en place et maintient une Politique de Sécurité du Système d'Information (PSSI) sur ses Systèmes d'Information en vue de réduire les risques liés à la sécurité.

La mise en œuvre de cette PSSI est pilotée par le Responsable de la Sécurité du Système d'Information (RSSI) du CNRS et est assurée par :

- les collaborateurs utilisateurs du Système d'Information ;
- le titulaire, au travers d'une PSSI spécifique et placée sous sa responsabilité ; les mesures à la charge du titulaire étant décrites dans la suite du chapitre.

3.1 PROCESSUS DE GESTION DE LA SECURITE

La gestion de la sécurité a pour but de s'assurer que les tous les moyens nécessaires sont mis en place pour respecter les besoins de sécurité des données dont la gestion est confiée au titulaire en termes de disponibilité, confidentialité, intégrité, traçabilité-auditabilité, quel que soit leur niveau de sensibilité.

Dans le cadre de la gestion de la sécurité, le titulaire doit assurer les tâches suivantes :

- l'élaboration d'un plan d'assurance sécurité (PAS) : ce document décrit les dispositions que le titulaire s'engage à mettre en œuvre pour répondre aux besoins de sécurité du CNRS. Il définit en particulier l'organisation mise en place, la méthodologie à suivre pour gérer la sécurité des prestations et les mesures techniques, organisationnelles et procédurales qui sont mises en œuvre.
- la mise en œuvre de ce plan pour les services qui lui sont confiés dans le périmètre de ce contrat ;
- l'organisation de sa propre veille de la sécurité ;
- la prise en compte des alertes de sécurité ;
- la participation à la gestion de crise du CNRS et aux plans de crise nationaux ;
- et de manière générale l'ensemble des activités de sécurité décrites dans ce chapitre.

Les livrables attendus du processus de gestion de la sécurité sont a minima :

- PAS – Plan d'assurance sécurité
- un tableau de bord trimestriel, à chaque comité sécurité
- suivi des alertes et des vulnérabilités de sécurité
- suivi des comptes et des droits
- rapports suite à tout incident de sécurité.

3.2 PSSI ET DECLINAISON PAS (PLAN D'ASSURANCE SECURITE)

Référence	Libellé exigence	Priorité
SSI_001	Pendant toute la durée de l'accord-cadre, le titulaire doit formaliser, maintenir à jour, appliquer et contrôler la mise en œuvre de la PSSI pour le périmètre placé sous sa responsabilité notamment par le (Plan d'Assurance Sécurité) PAS et les normes adéquates.	0
SSI_002	Le titulaire décline la PSSI mise en œuvre par la matérialisation d'un Plan d'Assurance Sécurité (PAS) opérationnel.	0
SSI_003	Toute modification de la PSSI du titulaire fait l'objet d'une validation par le CNRS.	0

3.3 SENSIBILITÉ DES DONNÉES

Le CNRS confie au titulaire l'opération d'un ensemble de prestations et de services qui l'amènent à manipuler des données qui relèvent du règlement européen sur la protection des données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Référence	Libellé exigence	Priorité
SSI_004	Les risques spécifiques liés à l'application sont l'atteinte en confidentialité et en intégrité sur les données, par des sources de menaces internes (malveillance, maladresse) ou externes. Le titulaire doit prendre toutes les mesures nécessaires pour diminuer la vraisemblance et/ou l'impact des risques listés. Le niveau maximal de sensibilité des données atteint au maximum le niveau Diffusion Restreinte.	0
SSI_005	Le CNRS interdit formellement tout transfert de données par le titulaire à un tiers, sans son information et son accord préalable, qu'il s'agisse de données de production, de test, auxiliaires à la prestation, de quelque nature que ce soit. Ceci vaut également pour toute communication de données sur demande d'une autorité judiciaire, française ou étrangère. Toutefois, le titulaire est délié de cette obligation dans le cas où il serait amené à faire cette communication sur ordre d'une autorité judiciaire française et que l'ordonnance lui interdise de communiquer l'information au CNRS.	0
SSI_006	Le titulaire ne stocke pas de données du CNRS en local sur ses postes de travail.	0
SSI_007	Le titulaire doit indiquer les règles de marquage qu'il applique 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. Le marquage des supports de stockage de données est obligatoire (disque dur, bandes de sauvegardes, etc.). Ce marquage permet de signifier son personnel le niveau de protection et les mesures réglementaires à appliquer en ce qui concerne la communication, la diffusion, la reproduction, la conservation et la destruction des informations marquées Le marquage doit être visible à l'œil nu et adapté aux caractéristiques physiques des supports. Il doit permettre d'identifier le propriétaire des données sans ambiguïté. Le marquage comporte une identification et un timbrage, c'est-à-dire l'apposition de la mention du niveau de classification.	0
SSI_008	Le marquage comporte une identification et un timbrage, c'est-à-dire l'apposition de la mention du niveau de classification. Le titulaire assure la protection de la documentation du CNRS sur support papier quelque soient les locaux qu'il utilise, par des moyens adaptés au niveau de sécurité requis. Le titulaire décrit les mesures de protection qu'il applique au stockage documentaire physique de ses clients. Le titulaire doit s'assurer que les données techniques manipulées par son personnel (inventaire des composants logiciels et matériels de la Prestation, dossier d'architecture, matrice des flux, schémas d'architecture, documentation technique, procédures, guides d'implémentation, configuration, etc.) sont stockées dans l'outil de gestion de la documentation fourni par le titulaire avec un accès permanent pour le CNRS.	0

3.4 ORGANISATION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (SSI)

Référence	Libellé exigence	Priorité
SSI_009	L'organisation mise en place par le titulaire doit inclure une partie dédiée à la SSI, qui définit notamment : <ul style="list-style-type: none"> – les responsabilités internes et à l'égard des tiers ; – les modalités de coordination avec les autorités externes ; – les modalités d'application des mesures de protection. 	0

SSI_010	L'équipe comporte a minima : <ul style="list-style-type: none"> – Une personne de niveau hiérarchique supérieur formé et compétent en SSI capable de prendre des décisions dans la conduite du projet, responsable du respect des dispositions du PAS. – Une personne intégrée ou proche des équipes du titulaire en charge du projet, responsable de la mise en œuvre du PAS. 	0
SSI_011	Les procédures d'application des mesures sont portées à la connaissance de toutes les parties prenantes et les intervenants concernés.	0
SSI_012	L'organisation des responsabilités SSI chez le titulaire doit être réalisée de manière à assurer une séparation des rôles incompatibles et à éviter les conflits d'intérêt.	1
SSI_013	Le titulaire fait connaître à son personnel intervenant dans le cadre de la Prestation ses rôles et ses responsabilités en matière de sécurité ainsi que les clauses de confidentialité du contrat.	0
SSI_014	Le titulaire veille notamment à ce que son personnel intervenant dans le cadre de la Prestation respecte les dispositions concernant la sécurité telles que décrites dans le présent CCTP. Le titulaire indique comment son personnel a connaissance des dispositions du cahier des charges notamment concernant les besoins de sécurité.	0

3.5 RELATIONS AVEC LES TIERS

Référence	Libellé exigence	Priorité
SSI_015	Dans le cadre de la PSSI mise en œuvre, le titulaire doit inclure et formaliser une politique spécifique relative aux relations avec les tiers (sous-traitants en particulier) dans le cadre des contrats sous-jacents, l'appliquer et contrôler sa mise en œuvre. Cette PSSI doit être revue annuellement.	0
SSI_016	Le titulaire doit également intégrer dans la PSSI les aspects relatifs à la sécurité, notamment en matière de confidentialité, dans les contrats passés avec les tiers dans le cadre des contrats sous-jacents.	0

3.6 PROCESSUS DE GESTION DES INCIDENTS DE SÉCURITÉ

Le plan d'assurance sécurité (PAS) définit les modalités de traitement des incidents de sécurité. Un incident de sécurité correspond à un ou plusieurs événements intéressant la sécurité de l'information, indésirable(s) ou inattendu(s), présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité (confidentialité, intégrité, disponibilité) de l'information. L'incident de sécurité peut impacter des actifs, des personnes, des processus...

Pour tout incident de sécurité, le Responsable de la sécurité du titulaire ou le Responsable du contrat prend attache avec le RSSI de la DSI du CNRS qui coordonne les actions à conduire en réaction à l'incident.

Les livrables attendus du processus de gestion des incidents de sécurité sont à minima :

- Mise en œuvre de l'outil de gestion des tickets d'incidents de sécurité ;
- Tickets saisis, renseignés, et clos selon les niveaux de service ou le planning défini

Référence	Libellé exigence	Priorité
SSI_017	Une coordination est mise en place entre les équipes sécurité du CNRS et les équipes du titulaire. Le CNRS donne instruction au titulaire d'agir seul ou en collaboration avec ses équipes pour les mesures de remédiation. Le retour d'expérience sur incident et le traitement des éventuelles causes profondes relève d'un pilotage par le comité SSI.	0

SSI_018	Le titulaire informe sans délai le CNRS de tout constat d'attaque ou d'intrusion, afin de pouvoir déclencher immédiatement toutes les actions nécessaires : chaque partie met à disposition de l'autre une liste de contacts de crise, joignables 24x7, dont l'information mutuelle immédiate est nécessaire au bon traitement des incidents.	0
SSI_019	La gestion des incidents est pilotée par le CNRS en coordination avec le titulaire. Ce dernier applique les décisions du CNRS, sans diminution de son devoir de conseil et d'alerte. Le titulaire peut également être amené à prendre lui-même des mesures conservatoires d'urgence qu'il estime nécessaire pour limiter la portée de l'incident : dans ce cas, il informe le CNRS le plus rapidement possible du contenu et des conséquences de ces mesures. Dans le cas où la portée de l'incident le nécessite, l'incident sera traité par une cellule de crise du CNRS.	0
SSI_020	Le titulaire maintient une base de connaissance des problèmes techniques. Le titulaire l'utilise pour tirer parti des connaissances recueillies suite à l'analyse et la résolution des incidents liés à la sécurité de l'information pour réduire la probabilité ou les conséquences d'incidents ultérieurs.	0
SSI_021	Le titulaire participe activement à toutes les actions forensiques ou de collecte d'informations demandées par le CNRS ou les autorités judiciaires.	0
SSI_022	Le service de supervision du titulaire comprend un système de remontée d'alerte afin de détecter tout comportement anormal lié à la volumétrie sur un périmètre SI lié à la prestation (ex : montée en charge du réseau). Les alertes sont remontées au SOC et/ou au NOC du titulaire.	0
SSI_023	Le titulaire doit assurer la traçabilité des incidents de sécurité et doit disposer d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur le périmètre de la prestation. Les vols d'ordinateurs, y compris les ordinateurs portables du titulaire, ou d'équipement nomades s'ils contiennent des informations concernant le CNRS, d'équipement ou de supports de données sont considérés comme des incidents de SSI et traités comme tels. Le titulaire ne peut communiquer d'information qu'aux seuls intervenants ayant « besoin d'en connaître » chaque fois que nécessaire.	0
SSI_024	Le titulaire devra respecter les plans gouvernementaux, et notamment renforcer ses contrôles d'accès physiques et logiques à ses équipements, si le CNRS lui en donne l'instruction. Dans le cadre de plans de sécurité gouvernementaux (y compris les exercices), le CNRS pourra demander une augmentation de la fréquence des sauvegardes.	0

3.7 DISPOSITIF DE SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Référence	Libellé exigence	Priorité
SSI_025	Le titulaire doit définir au sein de ses sites et locaux d'exécution des prestations, des zones de sécurité.	0
SSI_026	Le titulaire doit maintenir et appliquer des mécanismes de contrôle d'accès physique appropriés et adéquats pour empêcher tout accès non autorisé aux installations du titulaire conformément aux meilleures pratiques de sécurité.	0
SSI_027	Le titulaire doit formaliser et diffuser à l'ensemble des personnels intervenant dans les zones de sécurité, les consignes relatives au travail dans ces zones.	0
SSI_028	Le titulaire met en place des dispositifs protégeant les bureaux, salles et autres locaux d'exécution des prestations contre les risques d'intrusion, de captation d'information, de dégradation.	0
SSI_029	Le titulaire veille à ce que tout tiers ayant besoin d'un accès pour fournir un soutien ou une maintenance à tout équipement directement ou indirectement impliqué dans la fourniture des services soit connecté et déconnecté des installations du titulaire.	0

3.8 CONTRÔLE DES ACCÈS LOGIQUES

Les comptes concernés par ces exigences concernent les accès et comptes sous maîtrise du titulaire.

Référence	Libellé exigence	Priorité
SSI_030	Le titulaire doit formaliser et mettre en œuvre une politique de contrôle d'accès logique afin de gérer le cycle de vie des comptes d'accès et la gestion des habilitations.	0
SSI_031	La politique de contrôle des accès logiques couvre les accès aux réseaux et aux services réseaux, aux outils et plus largement à l'ensemble du périmètre applicatif et technique.	0
SSI_032	Lorsque le titulaire se voit accorder un accès logique, il le fera en utilisant une communication sécurisée et uniquement à partir d'une gamme d'adresses réseau désignées et pré-convenues du titulaire. Plus largement, le titulaire mettra en place un contrôle sécurisé des liens entre le titulaire et ses prestataires et/ou cotraitants L'accès autre que strictement nécessaire à l'accomplissement de ses obligations au titre de l'accord-cadre est strictement interdit.	0
SSI_033	Des mécanismes permettant de limiter les services, les données, les privilèges auxquels a accès l'utilisateur ou l'administrateur en fonction de son rôle dans l'organisation, sont mis en œuvre.	0
SSI_034	Les procédures d'attribution et la modification des accès et privilèges d'un service doivent être validés par le CNRS. Il importe de bien différencier les différents rôles et de n'attribuer que les privilèges nécessaires. Un inventaire régulièrement mis à jour est mis régulièrement à disposition du CNRS.	0
SSI_035	Le titulaire indique les mesures de contrôle discrétionnaire des accès logiques qu'il met en œuvre sur ses sites.	0
SSI_036	Il décrit les processus qu'il met en œuvre pour permettre au CNRS de valider les autorisations d'accès aux ressources faisant l'objet de la prestation.	0

3.9 INTERCONNEXION SITE TITULAIRE ET CNRS

Référence	Libellé exigence	Priorité
SSI_037	Le titulaire doit garantir l'utilisation d'un canal de communication réseau sécurisé entre ses ressources et celles du CNRS (chiffré, authentifié).	0
SSI_038	Le titulaire doit garantir, pour l'accès en mobilité (y compris télétravail) de ses collaborateurs une utilisation systématique et obligatoire d'un tunnel VPN sécurisé du titulaire. Ces accès en mobilité sont subordonnés à la fourniture des dossiers Sites Sûr et Plan d'Assurance Sécurité (PAS) complets et exhaustifs.	0

3.10 CONTRÔLE ET CONFORMITÉ

Référence	Libellé exigence	Priorité
SSI_039	Le titulaire doit s'assurer de sa conformité à la législation sur la propriété intellectuelle	0
SSI_040	Le titulaire doit mener lui-même ou en s'appuyant sur des tiers spécialisés parmi la liste des Prestataires d'audit de la sécurité des systèmes d'information (PASSI) de l'ANSSI, des audits de conformité avec les standards, la PSSI du titulaire et le Plan d'Assurance Sécurité en vigueur.	1
SSI_041	Le titulaire doit mener lui-même ou en s'appuyant sur des tiers spécialisés parmi la liste des PASSI de l'ANSSI, des audits de conformité technique, des audits de sécurité ou des tests d'intrusion	0
SSI_042	Le titulaire transmet les résultats des audits et des tests d'intrusion ainsi que les Plans d'Actions associés au CNRS.	0
SSI_043	Le titulaire doit dès le démarrage présenter le plan d'audit (annexe du Plan d'Assurance Sécurité PAS) envisagé en tenant compte des audits et certifications mises en place.	0

3.11 EXIGENCES LIÉES AUX DÉVELOPPEMENTS

L'application se doit de réduire au maximum les risques d'intrusion et de prévenir les stratégies d'attaques potentielles venant du web.

L'application ne doit pas être sensible à ce type de risques connus (liste non-exhaustive) :

- les injections de codes (de tous types : SQL, XML, Null Byte, LDAP, Mail Command, OS Command, XQuery...) ;
- les attaques par XSS (Cross Site Scripting) ;
- les attaques par des faiblesses dans la gestion des droits et des sessions ;
- les attaques par références directes aux objets ;
- les attaques par « Cross-Site Request Forgery » ;
- les attaques basées sur des erreurs de configuration ;
- les attaques sur des failles de restriction d'URL ;
- les attaques sur des URL d'accès aux objets prévisibles ;
- les attaques sur des redirections abusives.

Pour cela, l'application intègre, au moins, les dispositifs suivants :

Référence	Libellé exigence	Priorité
SSI_044	Le framework utilisé dispose d'un historique clair et vérifiable de ses vulnérabilités. A date d'implémentation, il ne présente pas de faille non corrigée. L'historique permet d'évaluer la réactivité de correction et la fréquence des failles, et est un argument du choix.	0
SSI_045	Lorsque l'analyse de risque en détermine la nécessité, le chiffrement des données est à mettre en place. Les outils et/ou protocoles de chiffrement utilisés sont qualifiés et certifiés par l'ANSSI.	0
SSI_046	Validation des entrées utilisateur : toute saisie utilisateur est vérifiée côté serveur en conformité avec le format, la taille, la sémantique et le type de données attendu.	0
SSI_047	Audit statique de code : le cycle de développement inclut des phases régulières d'audit statique de code, par l'utilisation d'outils d'aide à l'analyse et/ou par revue de code par un pair. Le titulaire fournit au CNRS les états réguliers de cette analyse.	0
SSI_048	Déconnexion à temps contraint paramétrable : l'utilisateur de la solution est déconnecté de sa session après un temps paramétrable dans la solution. Cette durée est implémentée de manière cohérente dans l'ensemble des modules techniques nécessaires à la solution.	0
SSI_049	Les identifiants de session utilisateur sont aléatoires avec entropie d'au moins 128 bits.	0
SSI_050	L'attribut Secure est associé au cookie de l'identifiant de session utilisateur.	0
SSI_051	L'attribut HttpOnly est associé au cookie de l'identifiant de session utilisateur.	0
SSI_052	Les informations liées aux habilitations des utilisateurs ne sont jamais passées en paramètres des URL.	0
SSI_053	Gestion des erreurs applicatives : les messages d'erreur applicatifs sont présentés à l'utilisateur en masquant toute information technique divulguant les composants de la solution et leurs versions.	0
SSI_054	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le téléversement est effectué dans une zone disque tampon, puis le fichier est déplacé hors de l'arborescence d'hébergement web.	1
SSI_055	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification du fichier repose sur le type MIME (sans faire confiance ni à l'extension du fichier ni aux entêtes HTTP reçues) et la taille du fichier. En cas de discordance le fichier est refusé.	1
SSI_056	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification de la présence de logiciels malveillants est réalisée par un dispositif de lutte contre les codes malveillant	0
SSI_057	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le nom du fichier téléchargé est anonymisé.	1

SSI_058	Gestion des vulnérabilités : une surveillance des vulnérabilités applicatives est mise en place pendant la durée de la vie de la solution, et à la correction <i>pro bono</i> de celles-ci. Ces vulnérabilités peuvent toucher toutes les briques applicatives nécessaires à la solution.	0
SSI_059	Dans le cadre d'un développement spécifique, une licence logicielle est choisie par le CNRS conformément à ses besoins. Une référence à cette licence apparaît dans chaque fichier source produit.	0
SSI_060	En fonction des résultats de l'analyse de risques et/ou de l'analyse d'impact sur la protection des données (AIPD) menées, les données stockées sont chiffrées au repos (at rest) selon les dispositions du RGS Annexe B2 (https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/). Les clés de chiffrement sont stockées de manière à n'être disponibles que pour les personnels ayant besoin d'en connaître. Dans certains cas, les administrateurs techniques et fonctionnels peuvent ne pas avoir accès aux données.	0
SSI_061	La solution prend en compte les besoins d'archivage numérique intermédiaire de ses données, selon les durées d'utilité spécifiées par la MOA/Archiviste. Quand cela est possible, elle implémente un connecteur vers le SAE intermédiaire transverse du CNRS.	1
SSI_062	Conformément au RGPD, quand le traitement réalisé par la solution relève d'un consentement de l'utilisateur, la solution se charge de vérifier l'existence de ce consentement.	0
SSI_063	Pour protéger les données, les environnements hors production n'utilisent pas les informations des données de production sauf dérogation expresse du CNRS.	0
SSI_064	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité couvrent au niveau de détail requis par la réglementation les activités de connexions et les opérations importantes menées sur ces systèmes quelle que soit la source (utilisateur, administrateur, scripts ou processus particulier) afin d'identifier l'auteur et la substance d'une action illicite, délictueuse, ou criminelle.	0
SSI_065	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont établis dans un format structuré dont les champs couvrent a minima pour chaque événement, requête ou action : <ul style="list-style-type: none"> - l'horodatage - le compte utilisateur ou processus associé - l'adresse IP ou la source à l'origine [en cas d'interaction distante] - le libellé intelligible de l'événement ou l'action - le code retour de l'action [option] - un identifiant unique de corrélation [option] - la taille de la requête [option] 	0
SSI_066	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont tous horodatés de manière fiable et synchronisés sur une même source temps en indiquant notamment le fuseau horaire si les journaux ne sont pas établis en heure UTC.	0
SSI_067	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont exportés en temps réel hors du système générateur, de manière fiable et intègre vers un système central de collecte accessible par le CNRS.	0

3.11.1 Auditabilité

Niveau de traçabilité

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

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

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

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

Gestion des traces

La solution doit permettre un reporting sur les :

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

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

3.11.2 Gestion des modules Drupal

Le titulaire utilisera en priorité les modules contribués, supportés par la communauté Drupal, maintenus régulièrement, en veillant à en limiter le nombre. Les modules seront de préférence reconnus par la Security Team de Drupal.

Sur Drupal, une majorité de modules à jour techniquement, demeurent en version alpha ou bêta durant de longues périodes. Le CNRS accepte leur utilisation, même si l'objectif à terme n'est d'avoir que des modules « stables ».

Le choix des modules à intégrer est idéalement gouverné par :

- La réactivité de la communauté à l'origine du module (et sa taille)
- L'ancienneté du module et son historique en termes de sécurité
- Le rapport service rendu sur risque induit
- La facilité de mise à jour et l'impact sur la mise à jour des autres modules et du cœur Drupal. Certains modules étant plus structurant que d'autre, ou pouvant engendrer à terme des régressions et une dette technique.

Ces éléments sont présentés par le titulaire à l'appréciation du CNRS, afin d'éclairer son choix pour la liste des modules initialement proposés et pour chaque nouveau module proposé à l'intégration. En cas de refus par le CNRS, le titulaire propose un module alternatif pour le même service rendu. Le CNRS peut aussi décider d'abandonner la fonctionnalité.

Il veillera également à suivre les bonnes pratiques Drupal, notamment dans les développements spécifiques.

4 PROTECTION DES DONNÉES À CARACTERE PERSONNEL (RGPD)

Ce paragraphe décrit la politique de protection des données personnelles et les mesures techniques et organisationnelles applicables.

Il précise les engagements pris par le titulaire pour protéger les données personnelles dans le cadre de l'exécution des prestations conformément au présent accord-cadre. Le paragraphe présente les dispositions de nature « juridique » et les dispositions de sécurité, ces dernières étant précisées de manière spécifique au Chapitre Exigences de sécurité.

Les exigences décrites dans le présent paragraphe survivront à l'expiration ou à la résiliation de l'accord-cadre aussi longtemps que les Données à caractère personnel seront traitées par le processeur de données. En cas de conflit ou d'incohérence entre le présent paragraphe sur la protection des données et toute autre partie de l'accord-cadre, ce dernier sera prioritaire.

4.1 DÉFINITIONS

Les définitions suivantes sont conformes au règlement européen n°2016/679 sur la protection des données personnelles.

Données à caractère personnel :

Toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation (adresse IP), un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données de catégorie particulière dites sensibles :

Les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions philosophiques ou religieuses, l'appartenance syndicale, l'orientation sexuelle, les données de santé, les données biométriques qui permettent d'identifier une personne, les données génétiques, le numéro de sécurité sociale, les données d'infraction.

Traitement de données personnelles :

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion

Responsable de traitement :

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant :

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

4.2 POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES AU CNRS

Le CNRS a mis en place des mesures et l'organisation pour respecter l'ensemble des exigences liées à la protection des données personnelles conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du règlement européen n°2016/679 sur la protection des données personnelles.

La politique de protection des données est pilotée par la Déléguée à la protection des données du CNRS, qui s'appuie pour sa mise en œuvre dans le présent accord-cadre sur :

- La Direction des Systèmes d'Information
- Les collaborateurs au CNRS utilisateurs des systèmes d'information
- Le titulaire à travers une politique de protection des données personnelles.

4.3 ORGANISATION DE LA PROTECTION DES DONNÉES

Dans le cadre du présent accord-cadre, le CNRS est responsable des traitements de données personnelles. Ces derniers ont pour finalité la gestion des sites web administrés par le CNRS : fourniture et publication de contenus, gestion du fonctionnement et de la sécurité du site, exploitation et maintenance (tierce maintenance applicative, gestion des profils et des accès).

Le CNRS, pour ce qui le concerne, procède à l'information des personnes sur leurs droits d'accès, de rectification, d'opposition, de suppression conformément à l'article 12 du RGPD qui lui est applicable.

Le titulaire intervient en qualité de sous-traitant⁴ pour le traitement des données nécessaires dans le cadre des prestations du présent accord-cadre.

Les données à caractère personnel correspondent :

- à des données d'identification
- à des données liées à la vie professionnelle
- à des données de connexion.

Les personnes concernées sont les personnes liées au CNRS (agents CNRS ou non), au titulaire, toute personne visitant le Portail CNRS et ses sites satellites.

Si le titulaire considère qu'une instruction constitue une violation ou non-conformité au RGPD, il en informe immédiatement le CNRS.

Référence	Libellé exigence	Priorité
DCP_001	<p>Il est rappelé au titulaire le nécessaire respect strict de la législation de protection des données à caractère personnel en vigueur, que le titulaire agisse comme sous-traitant ou comme responsable de traitement au sens de la loi.</p> <p>En particulier, aucun transfert de données à caractère personnel, vers quelque destination que ce soit, par le titulaire sans information et accord exprès et préalable du CNRS ne sera toléré. Cette obligation s'applique également aux données générées par le titulaire pour l'accomplissement de la prestation.</p> <p>Dans le contexte du Règlement Général pour la Protection des Données personnelles, le titulaire agit :</p> <ul style="list-style-type: none"> - pour les traitements mis en œuvre par le titulaire, en tant que sous-traitant du CNRS, responsable de traitement - pour les traitements qu'il met en œuvre lui-même à l'appui des prestations, en tant que responsable de traitement. <p>Dans le premier cas, le titulaire assiste le CNRS dans la constitution des dossiers de preuve garantissant que le responsable de traitement a mis en œuvre les mesures de sécurité adéquates pour garantir la protection des données à caractère personnel confiées à son sous-traitant. A ce titre, il lui communique :</p> <ul style="list-style-type: none"> - l'ensemble des documents qu'il établit dans le cadre de ses obligations liées aux traitements de données sous-traités ; - toute autre information nécessaire au CNRS pour remplir ses propres obligations dès lors que cette demande est formalisée. <p>Dans le second cas, le titulaire atteste être en conformité avec le Règlement Général.</p>	0

⁴ Le terme « sous-traitant » s'entend conformément à l'article 28 du RGPD.

4.4 POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES DU TITULAIRE

Référence	Libellé exigence	Priorité
DCP_002	<p>Le titulaire garantit la mise en place en interne d'une politique appropriée en matière de protection des données. Cette politique comprend l'ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées.</p> <p>Cette politique indique les coordonnées du titulaire, celles de son/sa délégué/e à la protection des données (DPD), ainsi que les engagements du titulaire concernant le respect des principes énoncés par le règlement européen général sur la protection des données, au regard notamment :</p> <ul style="list-style-type: none"> - de la mise en œuvre de traitements licites - du respect des droits des personnes - des destinataires des données collectées - de la durée de conservation des données collectées - des mesures de sécurité des données <p>Le titulaire transmet au CNRS la politique de protection des données personnelles qu'il met en œuvre.</p>	0

4.4.1 Registre des traitements

Référence	Libellé exigence	Priorité
DCP_003	Le titulaire tient un registre des traitements de données à caractère personnel qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par tout prestataire d'audit désigné par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).	0

4.4.2 Formation des personnels

Référence	Libellé exigence	Priorité
DCP_004	Le titulaire doit assurer la formation de ses personnels à la protection des données personnelles. Il communique chaque année au CNRS la liste des formations dispensées (nature, dates).	1

4.4.3 Confidentialité

Les données exploitées et hébergées sont, pour partie des données à caractère personnel dont la sensibilité est forte au sens de la réglementation sur la protection des données personnelles.

Référence	Libellé exigence	Priorité
DCP_005	<p>Le titulaire veille à ce que les personnels autorisés à traiter les données à caractère personnel s'engagent à en respecter la confidentialité ou soient soumis à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.</p> <p>Le titulaire s'engage à n'utiliser et ne conserver les données transmises que pour les seules finalités définies dans l'accord-cadre.</p>	0

4.5 TRAITEMENT DES DEMANDES D'ACCÈS AUX DONNÉES

Référence	Libellé exigence	Priorité
DCP_006	Le titulaire ne peut, de sa propre autorité, rectifier, supprimer ou restreindre le traitement des Données à caractère personnel traitées pour le compte du CNRS, sauf sur instructions écrites du CNRS.	0
DCP_007	Le titulaire informe le CNRS dans les plus brefs délais (et en tout état de cause dans les cinq jours ouvrables suivant sa réception) de toute communication reçue d'une Personne concernée concernant les droits de cette Personne concernée d'accéder, de modifier ou de corriger les Données à caractère personnel et de se conformer à toutes les instructions du CNRS en réponse à ces communications.	0

4.6 RECOURS À DES SOUS- TRAITANTS

Référence	Libellé exigence	Priorité
DCP_008	Lorsque le titulaire fait appel à des sous-traitants au sens des articles 4 et 28 du RGPD, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants. Une contractualisation adaptée est établie entre le titulaire et ses sous-traitants conformément à l'article 28 du RGPD.	0
DCP_009	Le titulaire s'assure que ses sous-traitants présentent les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des dispositions en vigueur en matière de protection des données personnelles pour le présent accord-cadre.	0
DCP_010	Le titulaire communique au CNRS la liste exhaustive des sous-traitants auxquels il fait appel pour la réalisation des prestations du présent accord-cadre. Il indique les noms et coordonnées des sociétés, l'objet de la prestation, les finalités de traitement, les catégories de données concernées, les lieux d'hébergement des données.	0
DCP_011	En cas de changement de sous-traitant ayant un impact sur les données à caractère personnel au titre du présent accord-cadre, le titulaire le notifie au CNRS avant le début des prestations. Le CNRS peut s'opposer à ce que le titulaire utilise ledit nouveau sous-traitant en notifiant le titulaire par écrit dans les dix (10) jours ouvrables suivant la réception de la notification du titulaire conformément au mécanisme décrit ci-dessus. Si le CNRS estime que le sous-traitant proposé ne satisfait pas au critère du présent accord-cadre, le titulaire propose sans surcoût au CNRS un nouveau sous-traitant qui respecte les contraintes du présent accord-cadre. Si le titulaire n'est pas en mesure de mettre à disposition une telle modification dans un délai raisonnable, qui ne doit pas dépasser trente (30) jours, le CNRS pourra résilier le présent accord-cadre uniquement pour les Services qui ne peuvent pas être fournis par le titulaire sans l'utilisation dudit nouveau sous-traitant en fournissant une notification écrite au titulaire.	0
DCP_012	Le recours à des sous-traitants ne dégage aucunement le titulaire de ses responsabilités au titre de l'exécution des prestations.	0

4.7 DURÉE DE CONSERVATION DES DONNÉES ET ARCHIVAGE

Référence	Libellé exigence	Priorité
DCP_013	Aucune donnée personnelle n'est conservée au-delà de la fin de l'accord-cadre (hors cas particulier des données de logs et archivages).	0
DCP_014	Le long de la durée de l'accord-cadre, les données de logs et d'archivages conservées respectent les dispositions précisées dans les § 1.7 Sauvegarde et § 1.8 Supervision. Le titulaire fournit, sur demande du CNRS, la preuve confirmant la mise en œuvre de ces durées de conservation.	0

DCP_015	Le long de la durée de l'accord-cadre, le titulaire supprime les comptes administrateurs définis au § 1.6.2 Accès et authentification des comptes administrateurs, sur demande du CNRS. Les données associées aux comptes administrateurs sont supprimées. Le titulaire fournit, sur demande du CNRS, la preuve confirmant les suppressions de ces comptes administrateurs et des données associées.	0
----------------	---	---

4.8 DESTRUCTION, RÉVERSIBILITÉ

Référence	Libellé exigence	Priorité
DCP_016	Lors de la résiliation ou à l'expiration de l'accord-cadre, ou sur demande écrite du CNRS à n'importe quel moment que ce soit, le titulaire devra, à ses propres frais, détruire tous les documents, et tout autre support pouvant contenir des Données personnelles, sans conserver aucune partie ou copie de ceux-ci. Un bordereau d'élimination devra être établi.	0
DCP_017	Le titulaire fournit au CNRS un Certificat de destruction des Données à caractère personnel sous une forme acceptable pour le CNRS, signé par un employé du titulaire qui a supervisé cette destruction.	0
DCP_018	Aucune copie ni doublon des Données à caractère personnel ne seront créées à l'insu du CNRS.	0

4.9 ANALYSE D'IMPACT SUR LA VIE PRIVÉE

Référence	Libellé exigence	Priorité
DCP_019	Le titulaire collabore avec le CNRS pour la réalisation des analyses d'impact sur la vie privée.	0

4.10 EXIGENCES DE SÉCURITÉ

Référence	Libellé exigence	Priorité
DCP_020	Le titulaire s'oblige à prendre toutes précautions utiles afin de protéger les données contre toute destruction accidentelle ou illicite, perte, altération, diffusion et de garantir que les données ne soient déformées, endommagées ou communiquées à des personnes non autorisées. Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité. Il met à la disposition du pouvoir adjudicateur toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le pouvoir adjudicateur ou tout auditeur dûment mandaté par lui. Le titulaire fournit un Plan Assurance Sécurité (PAS) qui intègre les dispositions pour la protection des données personnelles. Le titulaire prend les mesures de sécurité adaptées conformément aux exigences de sécurité du CNRS définies au chapitre 2.5.	0

4.11 TRAITEMENT DES INCIDENTS IMPACTANT LES DONNÉES À CARACTÈRE PERSONNEL

Référence	Libellé exigence	Priorité
DCP_021	Dès lors que dans le cadre d'un incident de sécurité, il est constaté une violation avérée ou potentielle des données ou des traitements des données à caractère personnel, le titulaire communique au CNRS dans les meilleurs délais, et sous 24 heures au plus tard après en avoir pris connaissance, la survenance de cette faille ou violation de sécurité ayant (ou pouvant potentiellement avoir).	0
DCP_022	Une fois cette communication effectuée, le titulaire fournit au CNRS notamment toute information relative à la nature de la violation, au nombre de personnes concernées, aux catégories et au nombre d'enregistrements de données à caractère personnel concernés, ainsi qu'aux conséquences probables de la violation, aux mesures prises pour y remédier et atténuer les éventuelles conséquences négatives.	0
DCP_023	Les incidents, failles et violations liés aux données ou au traitement des données à caractère personnel constituent des incidents de sécurité dont la gestion doit en être conforme.	0
DCP_024	Dans le cas d'un incident de sécurité très sévère (tel que défini par la CNIL), et à la demande du CNRS, le titulaire doit missionner un tiers indépendant pour une évaluation et un audit d'urgence de la faille de sécurité, et fournir au CNRS une copie complète de ce rapport.	0
DCP_025	Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la réglementation.	0
DCP_026	Le niveau de priorité accordé aux incidents de sécurité impactant les données à caractère personnel est automatiquement le niveau le plus élevé.	0
DCP_027	Le CNRS notifie à la CNIL, dans les meilleurs délais et si possible dans les 72 heures, toute violation de données à caractère personnel, sauf si, en fonction notamment des éléments transmis par le titulaire sur ladite violation, elle n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.	0
DCP_028	Lorsque la violation des données est susceptible d'engendrer un risque élevé pour les droits et libertés, le CNRS notifie aux personnes concernées ladite violation dans les meilleurs délais conformément à la réglementation.	0

4.12 AUDIT

Référence	Libellé exigence	Priorité
DCP_029	En complément des audits décrits au § 3.10 Contrôle et conformité SSI, le responsable du traitement dispose du droit de faire procéder à ses frais, par ses services ou tout tiers de son choix, à un audit du sous-traitant en vue de vérifier le respect par ce dernier de ses obligations au titre du présent document.	0

4.13 COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE

Référence	Libellé exigence	Priorité
DCP_030	Le CNRS et le titulaire s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information ou de contrôle.	0
DCP_031	Le titulaire informera le CNRS par écrit et dès que possible (mais au plus tard un (1) jour ouvrable à compter de la date d'une telle demande) de toute demande faite par un gouvernement, par un organisme chargé de l'application des lois et/ou des réglementations : <ul style="list-style-type: none"> - D'informations concernant le CNRS - D'accès aux Données Personnelles à moins que la notification au CNRS ne soit interdite par la réglementation Française. Le titulaire coopérera avec le CNRS pour répondre à ces demandes.	1

DCP_032	<p>Le CNRS doit être immédiatement informé des inspections et mesures effectuées par l'autorité de contrôle, dans la mesure où elles concernent le traitement des données à caractère personnel.</p> <p>Ceci s'applique également dans la mesure où le titulaire fait l'objet d'une enquête ou est partie à une enquête d'une autorité compétente en relation avec des infractions à toute loi civile ou pénale, ou règle ou réglementation administrative concernant le traitement des Données à caractère personnel en relation avec l'accord-cadre.</p>	1
----------------	--	---

5 ANNEXES

5.1 GLOSSAIRE

Le tableau suivant présente le glossaire des termes utilisés dans ce document.

Terme	Description
Authentification multifacteur	Méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.
Document applicable	Document devant être obligatoirement appliqué par le Titulaire
CCTP	Cahier des Clauses Techniques Particulières
Document de référence	Document pouvant être utilement consulté par le titulaire.
EAI/ESB	Plateforme d'intermédiation des flux de données.
Flux	Tout échange de données ou d'information entre deux briques applicatives (y compris services d'intermédiation), quelle que soit la modalité et forme de cet échange. Un flux peut être entièrement manuel, ou peut faire appel à des services web, ou peut passer par l'EAI/ESB, etc.
LDAP	<u>Protocole</u> permettant l'interrogation et la modification des services d'annuaire.
REST	Style d'architecture d'échange de données autour de services web basés sur le protocole HTTP
CTA (Call to Action)	Élément interactif (bouton, lien, bannière) incitant l'utilisateur à effectuer une action spécifique, comme s'inscrire, télécharger un document ou acheter un produit.
Shibboleth	Mécanisme de propagation d'identités, développé par le consortium Internet2 , qui regroupe 207 universités et centres de recherche. Pour toute information complémentaire se référer au site suivant : https://www.shibboleth.net/
Téléservice	Application destinée à la communication inter-administration ou destinée à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public.