

ASSISTANCE A L'ADMINISTRATION ET MAINTENANCE DES ÉQUIPEMENTS DU RÉSEAU SIREs

Cahier des Clauses techniques Particulières (CCTP)

Version : 2.0

Date : 16/07/25

Objet : Ce document détermine les besoins techniques et organisationnels associés à l'assistance à l'administration et maintenance des équipements du réseau SIREs

SOMMAIRE

SOMMAIRE	2
1 PRÉAMBULE	5
2 INTRODUCTION	6
2.1 Contexte	6
2.2 Objectifs du marché	6
3 DESCRIPTION DE L'ENVIRONNEMENT	7
3.1 Présentation du CNRS	7
3.2 Les instituts	7
3.3 Les unités (laboratoires)	7
3.4 Des tutelles et des financements potentiellement multiples	8
3.5 Des différences de taille	8
3.6 Des implantations géographiques diverses	8
3.7 La direction générale déléguée à la science (DGD-S)	8
3.8 La direction générale déléguée aux ressources (DGD-R)	8
3.9 La mission pilotage et relations avec les délégations régionales et les instituts (MPR)	9
3.10 La direction de la stratégie financière, de l'immobilier et de la modernisation (DSFIM)	9
3.11 La direction déléguée aux achats et à l'innovation (DDAI)	9
3.12 La direction des comptes et de l'information financière (DCIF)	10
3.13 La direction des ressources humaines (DRH)	10
3.14 La direction des systèmes d'information (DSI)	10
3.15 Les délégations régionales (DR)	11
3.16 Présentation du réseau du système d'information	12
3.16.1 Le système d'information du CNRS	12
3.16.2 Le réseau SIRES	12
3.16.3 Les équipements	16
4 PRÉSENTATION DU MARCHÉ ACTUEL	17
4.1.1 Organisation	17
4.1.2 Supervision	17
4.1.3 Exploitation	17
4.1.4 Suivi des alertes de sécurité	18
4.1.5 Maintenance	18
5 DÉFINITION DU BESOIN DU CNRS POUR LE NOUVEAU MARCHÉ	19
5.1 Généralités	19
5.2 Gouvernance du marché	19
5.2.1 Organisation	19
5.2.2 Gouvernance	20
5.2.3 Documentation	23
5.3 Caractéristiques des prestations techniques attendues	24
5.3.1 Prestation de maintenance	24
5.3.2 Prestation de supervision et traitement des incidents	25
5.3.3 Prestation d'exploitation	28
5.4 Outillage	32
5.4.1 Guichet unique	32
5.4.2 Portail de suivi	32
6 EXIGENCES DE SÉCURITÉ	33
6.1 Principes généraux	33

6.2	mesures de Sécurité	33
6.2.1	Gestion de la Sécurité par le titulaire	33
6.2.2	Sécurité du matériel	33
6.2.3	Gestion de l'exploitation	34
6.2.4	Contrôle d'accès	36
6.2.5	Maintenance des systèmes – Gestion des vulnérabilités techniques	36
6.3	Clauses de sécurité	37
6.3.1	Obligations du titulaire	37
6.3.2	Localisation des données	37
6.3.3	Engagement de confidentialité	37
6.3.4	Audits de sécurité	39
6.3.5	Application des plans gouvernementaux	39
6.3.6	Incident concernant les données à caractère personnel	39
7	DEFINITION DES PRESTATIONS.....	ERREUR ! SIGNET NON DÉFINI.
7.1	PRISE EN CHARGE	41
7.1.1	Contenu de la prestation	41
7.1.2	Modalités d'exécution	41
7.1.3	Livrables et reporting.....	41
7.1.4	Contrat de service	41
7.1.5	Pénalités	41
7.2	MAITRISE D'ŒUVRE DÉLÉGUÉE	42
7.2.1	Contenu de la prestation	42
7.2.2	Modalités d'exécution	42
7.2.3	Livrables et reporting.....	42
7.2.4	Contrat de service	42
7.2.5	Pénalités	42
7.3	RÉVERSIBILITÉ	43
7.3.1	Contenu de la prestation	43
7.3.2	Modalités d'exécution	43
7.3.3	Livrables et reporting.....	43
7.3.4	Contrat de service	43
7.3.5	Pénalités	43
7.4	MAINTENANCE	43
7.4.1	Contenu de la prestation	43
7.4.2	Modalités d'exécution	43
7.4.3	Livrables et reporting.....	43
7.4.4	Contrat de service	44
7.4.5	Pénalités	44
7.5	SUPERVISION DES ÉQUIPEMENTS ET DES VULNÉRABILITÉS	45
7.5.1	Contenu de la prestation	45
7.5.2	Modalités d'exécution	45
7.5.3	Livrables et reporting.....	45
7.5.4	Contrat de service	45
7.5.5	Pénalités	46
7.6	EXPLOITATION	47
7.6.1	Contenu de la prestation	47
7.6.2	Modalités d'exécution	47
7.6.3	Livrables et reporting.....	47
7.6.4	Contrat de service	47
7.6.5	Pénalités	47
7.7	CATALOGUE DE SERVICES.....	48
7.7.1	Intervention sur site SIREs	48
7.7.2	Services relevant de l'exploitation des équipements	48

7.7.3	Modalités d'exécution	49
7.7.4	Livrables et reporting.....	49
7.7.5	Contrat de service	49
7.8	EXPERTISES	49
7.8.1	Contenu de la prestation	49
7.8.2	Modalités d'exécution	49
7.8.3	Livrables et reporting.....	49
7.8.4	Contrat de service	49

1 PRÉAMBULE

Ce document a été construit dans le but de bien différencier les éléments de compréhension du contexte, l'expression des besoins CNRS et la définition des prestations qui structureront le marché. Cela induit une répartition des informations dans les différents chapitres et l'utilisation de fréquents renvois.

Aussi, et afin de faciliter la tâche du lecteur, cette présentation du document décrit les objectifs et le contenu de chacun des chapitres de ce cahier des charges.

§2 - Introduction

Ce chapitre introduit le document en décrivant le **contexte** et les **objectifs** du marché.

§3 - Description de l'environnement

Ce chapitre donne une vision générale de **l'organisation et du positionnement de la DSI** du CNRS et de son réseau.

§4 - Description de du marché actuel

Ce chapitre donne une **vision synthétique de l'architecture technique et du marché** existants qui vont permettre au titulaire d'évaluer les contraintes et les stratégies qui guident la DSI dans la gestion du réseau du Système d'information.

§5 – Définition du besoin du CNRS

Ce chapitre **définit le besoin** du CNRS pour ce marché, à l'exception de ceux relevant spécifiquement de la sécurité

§6 - Exigences de Sécurité

Ce chapitre complète la définition du besoin CNRS et reprend en détail les **exigences de sécurité** qui s'imposent au titulaire. Ces exigences sont déclinées en **principes** généraux, **mesures** de sécurité et **clauses** de sécurité.

§07 – Définition des prestations

Ce chapitre identifie et spécifie l'ensemble des **prestations** qui structurent le marché : un sous chapitre est réservé à chacune d'entre elles.

Pour chacune des prestations, on identifie le **contenu**, les **modalités d'exécution**, les **livrables** et les caractéristiques de **reporting**, ainsi que les éléments relatifs au **contrat de service**.

2 INTRODUCTION

2.1 CONTEXTE

La DSI du CNRS a en charge l'informatique de gestion de l'établissement. Elle définit et met en œuvre le système d'information correspondant et gère les infrastructures associées.

Le réseau SIREs a été créé pour permettre une communication stable et sécurisée entre les différents acteurs de ces systèmes d'information. Dans ce cadre, un marché d'administration, supervision et maintenance des équipements a été mis en place depuis une vingtaine d'années.

2.2 OBJECTIFS DU MARCHÉ

Le CNRS souhaite renouveler son marché d'infogérance du réseau SIREs.

Il souhaite mettre en place un marché lui permettant de :

- Assurer la supervision du réseau.
- Assurer l'exploitation du réseau.
- Assurer la maintenance des équipements.
- Avoir au travers de multiples indicateurs une vision précise du fonctionnement du réseau.
- Suivre les vulnérabilités pouvant affecter les équipements et les mettre à jour.
- Intégrer de possibles évolutions du réseau tant au niveau des services (Sécurité, VoIP, ToIP, IPv6, ...) que des équipements.
- Répondre à des besoins d'expertise ponctuels ou à d'autres prestations décrites dans la bibliothèque de services.

Le marché actuel arrive à échéance fin Mars 2026. Le titulaire prendra la responsabilité totale des prestations à compter du 1^{er} jour du mois suivant la notification du marché.

Les moyens de cette prise en charge auront dû être mis en place préalablement dans le cadre de la prestation qui lui est dédiée avec une priorité sur la reprise de la maintenance.

3 DESCRIPTION DE L'ENVIRONNEMENT

3.1 PRÉSENTATION DU CNRS

Le **Centre national de la recherche scientifique** est un organisme public de recherche (Établissement public à caractère scientifique et technologique, placé sous la tutelle du **Ministère de l'Enseignement supérieur et de la Recherche**). Il produit du savoir et met ce savoir au service de la société.

Sa gouvernance est assurée par le président du **CNRS**, assisté de deux directeurs généraux délégués, l'un à la science et l'autre aux ressources.

Avec près de 34 000 personnes (dont 25 300 statutaires - 11 300 chercheurs et 14 000 ingénieurs, techniciens et administratifs), un budget pour 2013 de 3,415 milliards d'euros dont 802 millions d'euros de ressources propres, une implantation sur l'ensemble du territoire national, le **CNRS** exerce son activité dans tous les champs de la connaissance, en s'appuyant sur plus de 1100 unités de recherche et de service.

Principal organisme de recherche à caractère pluridisciplinaire en France, le **CNRS** mène des recherches dans l'ensemble des domaines scientifiques, technologiques et sociétaux. Il couvre la totalité de la palette des champs scientifiques, qu'il s'agisse des mathématiques, de la physique, des sciences et technologies de l'information et de la communication, de la physique nucléaire et des hautes énergies, des sciences de la planète et de l'Univers, de la chimie, des sciences du vivant, des sciences humaines et sociales, des sciences de l'environnement ou des sciences de l'ingénierie. Le **CNRS** est présent dans toutes les disciplines majeures regroupées au sein de dix instituts dont trois sont nationaux.

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

Figure 1 : Organisation du CNRS

Des informations plus complètes sont disponibles sur le site Web, adresse : <http://www.cnrs.fr>.

3.2 LES INSTITUTS

Les instituts sont les structures de mise en œuvre de la politique scientifique de l'établissement. Les directeurs des instituts participent à l'élaboration de la politique scientifique du **CNRS** et définissent les modalités de son application.

Chaque institut anime et coordonne l'action d'un ensemble cohérent d'activités de recherche relevant de plusieurs disciplines. Des programmes interdisciplinaires de recherche intéressant plusieurs instituts peuvent être décidés par le président après avis du conseil scientifique et approbation du conseil d'administration.

3.3 LES UNITÉS (LABORATOIRES)

C'est au sein des laboratoires, ou unités de recherche, que sont remplies les principales missions de l'organisme. Ces unités, en général constituées d'équipes de recherche, forment la structure de base de l'établissement. Les unités de recherche « propres » du **CNRS** sont créées par décision du président, après avis du Comité national de la recherche scientifique. Des unités de recherche relevant d'organismes extérieurs peuvent être associées au **CNRS**. Elles sont alors dites « mixtes » (UMR) ou « associées » (URA) et leur tutelle scientifique est assurée conjointement par le **CNRS** et les établissements partenaires.

Le **CNRS** compte 1029 unités de recherche dont plus de 96% en partenariat avec près de 120 établissements d'enseignement supérieur et de recherche et autres organismes nationaux et internationaux.

Des unités de recherche **CNRS** sont également implantées à l'étranger, dont 22 unités mixtes internationales (UMI).

Le **CNRS** compte également 111 unités de service dont plus de 76% en partenariat (observatoires des sciences de l'Univers, Maisons des sciences de l'Homme...)

3.4 DES TUTELLES ET DES FINANCEMENTS POTENTIELLEMENT MULTIPLES

Une unité de recherche peut dépendre d'une ou plusieurs délégations du **CNRS** et/ou d'un ou plusieurs établissements d'enseignement supérieur (EPSCP - EPST – EPIC...), ce qui signifie, en particulier, que son budget peut être éclaté entre plusieurs tutelles administratives. Le **CNRS** et plusieurs établissements d'enseignement supérieur (jusqu'à 3 parfois) peuvent participer au financement d'un même laboratoire.

L'origine des ressources financières des laboratoires de recherche publics est multiple :

- le budget de l'état : les établissements d'enseignement supérieur et les organismes de recherche (**CNRS**, INSERM, INRA,)
- l'Europe
- l'ANR
- les collectivités territoriales
- les organismes et entreprises publics
- les organismes ou entreprises privés
- les associations.

3.5 DES DIFFÉRENCES DE TAILLE

Tous les champs disciplinaires sont couverts par les laboratoires. Leur effectif peut varier de quelques dizaines de personnes (20 personnes pour les petites unités de recherche) à plusieurs centaines de personnes (400 à 800 personnes pour les quelques grosses unités de recherche).

Le budget de fonctionnement et d'investissement (hors personnels payés sur budget de l'état) dépend de la taille du laboratoire et de son champ disciplinaire (de moins de 150 000 euros à quelques millions d'euros). La gestion d'un laboratoire est donc très dépendante de sa taille et de son budget : une équipe de gestion commune à plusieurs laboratoires, une secrétaire-gestionnaire dans certains laboratoires, une équipe de gestion dans les plus gros laboratoires.

3.6 DES IMPLANTATIONS GÉOGRAPHIQUES DIVERSES

L'implantation géographique des laboratoires est très diverse : campus appartenant au **CNRS**, campus universitaires, campus d'autres organismes de recherche, laboratoires isolés. Certains laboratoires sont composés d'équipes de recherche implantées sur des lieux géographiques différents (jusqu'à 3 ou 4 sites) qui peuvent être sur le même campus universitaire, ou dans la même ville, ou dans des villes différentes.

3.7 LA DIRECTION GÉNÉRALE DÉLÉGUÉE À LA SCIENCE (DGD-S)

La [direction générale déléguée à la science](#) conduit, aux côtés du président, la politique scientifique de l'établissement. Elle a en charge la coordination de l'action des dix instituts du **CNRS**, veille à promouvoir l'interdisciplinarité et organise les partenariats avec les divers acteurs de la recherche, à l'échelle régionale, nationale, européenne ou internationale. Dans ce cadre, et en relation étroite avec [la direction générale déléguée aux ressources](#) (DGD-R), elle s'appuie sur les compétences des délégations régionales.

Des informations plus complètes sont disponibles sur le site Web, à l'adresse suivante :

3.8 LA DIRECTION GÉNÉRALE DÉLÉGUÉE AUX RESSOURCES (DGD-R)

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

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

3.9 LA MISSION PILOTAGE ET RELATIONS AVEC LES DÉLÉGATIONS RÉGIONALES ET LES INSTITUTS (MPR)

La **MPR** assure le pilotage transverse de la DGD-R.

Elle coordonne l'ensemble des relations avec les délégations régionales.

Elle garantit le lien entre les entités de la DGD-R, et celles de la DGD-S, et notamment la coordination avec les instituts.

Elle a notamment pour rôle de :

- piloter les projets transversaux de l'administration,
- garantir le lien entre les directions fonctionnelles de la DGD-R du **CNRS**, celles de la DGD-S, les délégations régionales et les instituts pour les actions nationales de l'administration,
- assurer la coordination de la production, de la gestion et de la diffusion de l'information administrative de l'établissement,
- initier et accompagner la simplification et l'ingénierie des processus administratifs,
- faire connaître et valoriser les actions de l'administration.

La MPR est composée de 3 pôles distincts :

- le pôle pilotage
- le pôle Affaires européennes
- le pôle Coordination et information

3.10 LA DIRECTION DE LA STRATÉGIE FINANCIÈRE, DE L'IMMOBILIER ET DE LA MODERNISATION (DSFIM)

La **DSFIM** a pour missions :

- d'assurer la programmation, la préparation et l'exécution du budget, en faisant le lien entre l'allocation des ressources et la réalisation des objectifs,
- de l'optimisation des ressources, de la modernisation de la gestion,
- de la mise en œuvre de la stratégie patrimoniale.

La DSFIM a en charge la prospective et la mise en œuvre des orientations stratégiques dans son domaine.

Elle anime le réseau des correspondants budgétaires et financiers du **CNRS**.

3.11 LA DIRECTION DÉLÉGUÉE AUX ACHATS ET À L'INNOVATION (DDAI)

Intégrée au sein de la Direction de la Stratégie Financière de l'Immobilier et de la Modernisation (DSFIM) du **CNRS**, la DDAI a en charge les missions suivantes :

- formuler les propositions relatives à la politique d'achat de l'établissement, participer à son élaboration et à sa mise en œuvre,
- assurer la passation et l'exécution des marchés publics nationaux pour les domaines d'achat relevant de sa compétence,
- accompagner la déconcentration et la coordination des achats.

A ce titre, le Directeur et son équipe ont en charge :

- la veille technologique des produits et matériels utilisés par les unités de recherche,
- l'identification et l'évaluation des besoins des unités du **CNRS**,
- le choix du mode de passation et de dévolution des marchés publics,
- le suivi du bon déroulement des procédures dans le respect des textes en vigueur,
- la sélection des candidatures et des offres les mieux adaptées aux besoins des unités du **CNRS**,
- le suivi de la bonne exécution des marchés publics.

La DDAI assure également un rôle d'animation auprès des acheteurs en Délégations (mission de conseil, de formation et d'information réglementaire).

Dans le cadre de ses activités, la DDAI est en relation permanente avec les autorités de contrôle et les autres organismes de recherche.

3.12 LA DIRECTION DES COMPTES ET DE L'INFORMATION FINANCIÈRE (DCIF)

La **DCIF** est garante de la régularité des opérations comptables et de la cohérence de l'ensemble des informations financières et comptables. Elle assure le suivi et l'enregistrement des actes de gestion liés à la mise en œuvre des crédits et à l'exécution du budget. Elle garantit l'exhaustivité et la qualité des données. Elle restitue l'information financière selon les besoins et les calendriers des services utilisateurs, de la direction de l'établissement ou des tutelles.

Dans son domaine, elle est en charge de la maîtrise d'ouvrage des systèmes d'information ainsi que de l'administration des données. Elle est la principale maîtrise d'ouvrage de l'application GESLAB.

3.13 LA DIRECTION DES RESSOURCES HUMAINES (DRH)

La **DRH** est chargée d'élaborer et de mettre en œuvre la politique de gestion des ressources humaines du **CNRS**. Celle-ci s'articule autour de quatre grands domaines :

- Gestion collective : suivi et gestion prévisionnelle des emplois et compétences ;
- Gestion individualisée des personnels, depuis leur recrutement jusqu'à leur départ, s'agissant tant du suivi de leur vie professionnelle quotidienne que de leur parcours de carrière ;
- Valorisation des ressources humaines : l'organisation du travail, le développement des compétences, les conditions de travail ;
- Mise en place et suivi d'une politique sociale : fonctionnement des instances, contacts avec les représentants du personnel, articulation entre la vie personnelle et la vie professionnelle...

Les responsabilités directes de gestion s'exercent au sein des services des ressources humaines (SRH) des délégations régionales. Ces services assurent la gestion administrative des personnels, la formation, le conseil en RH et garantissent un service social aux agents.

3.14 LA DIRECTION DES SYSTÈMES D'INFORMATION (DSI)

La direction des systèmes d'information (DSI) définit, met en place et gère les moyens techniques nécessaires aux systèmes d'information et de communication de l'établissement.

La DSI a en charge :

- le maintien et l'optimisation de la performance des réseaux informatiques et des télécommunications,
- la définition et la mise en œuvre des systèmes d'information (SI) destinés au pilotage et à la gestion des activités de l'établissement,
- le développement d'outils et services à destination des laboratoires,
- le développement des synergies entre les plates-formes informatiques du **CNRS** et de ses filiales,
- de contribuer au développement d'actions communes décidées entre l'établissement et ses partenaires,
- la planification des évolutions dans le cadre d'un schéma directeur.

Elle coordonne et anime le réseau des informaticiens des services et des laboratoires rattachés au **CNRS**.

Les systèmes mis en œuvre accompagnent les processus de support et de pilotage de la recherche scientifique et touchent une grande diversité d'activités allant par exemple de la gestion et la paie du personnel **CNRS**, à la gestion budgétaire, financière et comptable de l'établissement ainsi qu'à la gestion des opérations de partenariats de recherche. Ces systèmes sont élaborés pour les laboratoires, les délégations et les directions administratives et scientifiques du **CNRS**.

La DSI comprend :

- **La Direction** : la directrice, un directeur adjoint et une directrice adjointe administrative.
 - Le Secrétariat Général : il est chargé des aspects administratifs de la DSI. Il gère les ressources humaines, le budget, le contrôle de gestion, la logistique et les achats.
 - Les départements Applications et services :
 - **SI finance**
 - **SI ressources humaines et paie**
 - **SI laboratoires et soutien à la recherche**
 - **SI ressources humaines, santé prévention sécurité, décisionnel**
 - Les départements Organisation et support :
 - **Sécurité SI**
 - **Plateformes des référentiels et de dématérialisation**
 - **Architecture et assistance applicatives**
 - **Infrastructures SI**
 - **Sites web, communication, accompagnement projet**

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

Pour d'autres informations, il est possible de consulter le site Web de la DSI à l'adresse suivante :

<http://www.dsi.cnrs.fr/>

3.15 LES DÉLÉGATIONS RÉGIONALES (DR)

Le **CNRS** est organisé territorialement en 17 délégations, placées chacune sous la responsabilité d'un délégué régional. Il représente la direction générale en région.

Les délégations assurent une gestion directe et locale des laboratoires et entretiennent les liens avec les partenaires locaux et les collectivités territoriales.

Pour d'autres informations, il est possible de consulter les sites web du **CNRS** en région à l'adresse suivante : <https://www.cnrs.fr/fr/delegations-regionales-du-cnrs>

3.16 PRÉSENTATION DU RÉSEAU DU SYSTÈME D'INFORMATION.

3.16.1 Le système d'information du CNRS

La Direction des systèmes d'information du CNRS met en place et maintient les applications de gestion du CNRS.

Ces applications servent deux grands axes du Système d'information du CNRS :

- Les ressources humaines : gestion des personnels, paie
- Les finances : gestion du budget et des affaires comptables et financières.

Ces applications sont en infogérance auprès d'un groupement de prestataires qui assure l'hébergement, la gestion des systèmes et la MOA.

Toutes les autres applications et services du Système d'Information du CNRS sont développés par des prestataires externes, mais mises en œuvre et exploitées par la DSI du CNRS. Ces applications sont hébergées dans des centres serveurs, soit privés, soit appartenant au CNRS.

Elles sont essentiellement accessibles en client léger depuis les délégations et laboratoires du CNRS réparties sur tout le territoire.

3.16.2 Le réseau SIRES

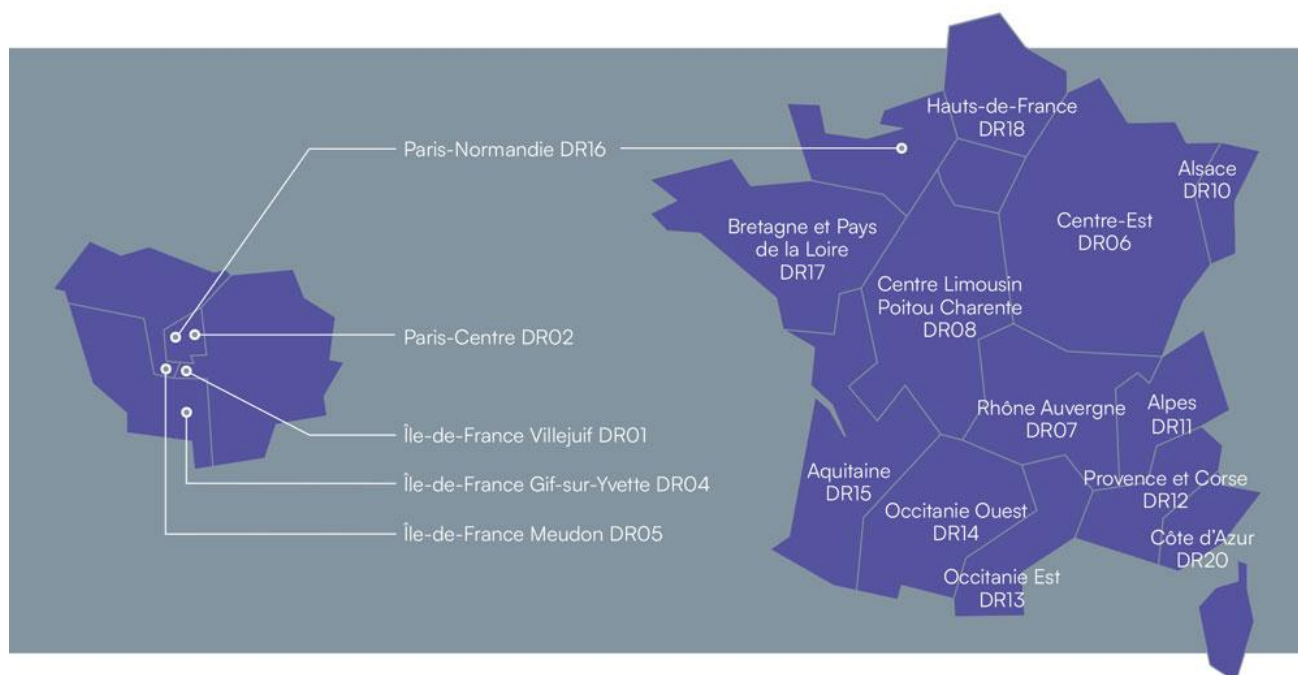
Les flux liés aux applications de gestion du CNRS transitent par le réseau SIREs.

C'est le réseau national dédié au système d'information du CNRS, exploité en 24h/24 7/7 par le titulaire du marché.

Les sites concernés par un raccordement à SIREs sont :

- Les 17 sites des délégations régionales du CNRS, sites géographiquement répartis sur l'ensemble des régions administratives du territoire national, (cf. lien §3.15)
- Le siège du CNRS.
- Le service de cloud hébergeant les applications liées au progiciel SAP.
- Le centre serveur hébergeant la messagerie du CNRS ainsi que diverses offres de services à destination des laboratoires.
- Le site du centre de calcul de l'IN2P3 (Villeurbanne) qui héberge la majorité des d'applications du SI.
- Les sites de la Direction des systèmes d'information (DSI) à Labège (31) et Meudon (92).

D'autres sites ou Centres serveurs pourront être intégrés au cours du marché.



L'infrastructure réseau qui relie ces sites s'appuie, selon les cas, sur un ensemble de réseaux qui sont autant d'entités administrées de manière autonome.

Ces réseaux sont :

- Le réseau local de l'unité (Délégation Régionale, centre serveur, ...), administré par son « service système et réseau ». Ce service est chargé de la gestion de proximité des équipements (administrateurs informatiques...)
- Le réseau du campus sur lequel est situé l'unité (campus CNRS ou universitaire) ; il est administré par le « service réseau du campus » qui peut être le même que celui de l'unité.
- Le réseau métropolitain et/ou régional (appelé « réseau de collecte ») ; son exploitation est généralement sous-traitée, en tout ou partie, à une société de services.
- Le réseau national RENATER, dont l'exploitation est assurée par le NOC Renater et l'équipe SSO (Service de Suivi Opérationnel) du GIP Renater.

Le Réseau national RENATER



Le cheminement des communications entre les différentes entités de SIRes n'est pas uniforme. Elles peuvent, en effet, traverser tout ou partie de ces réseaux.

Le raccordement au réseau de collecte ou à Renater peut également s'effectuer au travers d'une liaison spécialisée louée à un opérateur.

Dans tous les cas, Renater fournit un accès à son service L3VPN (https://services.renater.fr/_media/vpn/doc-l3vpn.pdf) dans les nœuds de raccordement proches des sites SIRes.

Les sites sont raccordés à l'équipement Renater via un ou plusieurs VLans (N2).

Pour le service d'Hébergement cloud, la liaison au réseau SIRes se fait au travers de deux VPN ipsec entre le centre serveurs du prestataire « SecNumCloud » et deux sites SIRes.

L'ensemble des utilisateurs finaux utilisant SIRes quotidiennement représente environ 2700 utilisateurs.

Les 1500 unités de recherche du CNRS bien que n'étant pas intégrées au réseau SIRes peuvent être amenées à utiliser les applications hébergées sur les centres serveurs du CNRS. (Entre 30 000 et 150 000 utilisateurs).

Les objectifs de SIRes sont, d'une part, d'assurer une partie de la sécurité des sites et, d'autre part, de garantir la qualité du service d'accès aux applications avec, entre autres, la stabilité des temps de réponse pour l'ensemble des communications et une disponibilité maximale du service réseau.

Sur le réseau SIRes transitent :

- Tous les flux entre les différents sites en adressage privé et public.

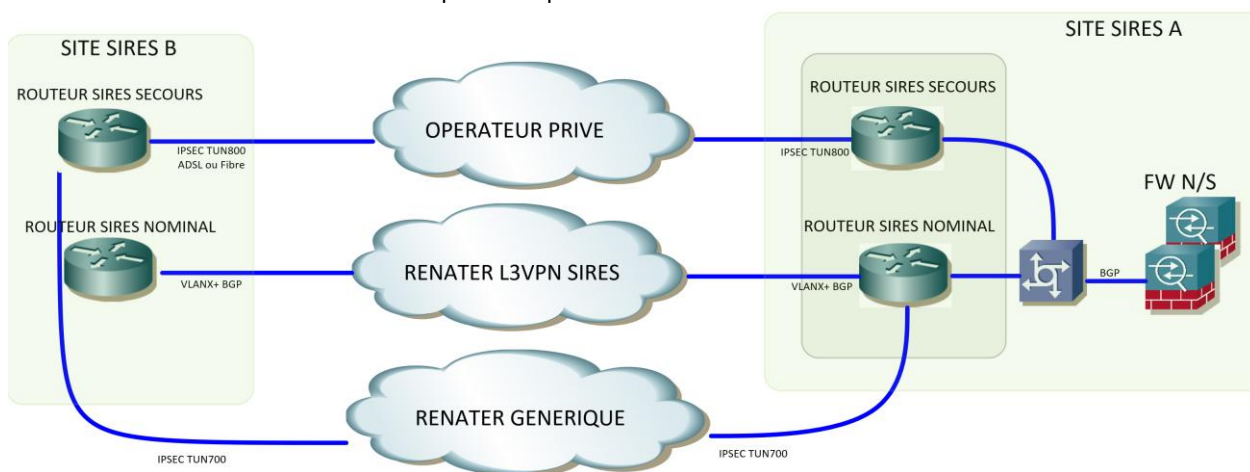
Des mécanismes de redondance sont prévus en cas de panne :

- L'accès réseau étendu est doublé sur les centres serveurs d'Elancourt et de Villeurbanne (IN2P3).
- Chaque site dispose d'un routeur de secours et à minima d'une liaison de secours ADSL (une évolution vers de la fibre est en cours)

Chaque site dispose d'un moyen de filtrage des flux :

- Des firewalls sont en place sur tous les sites.
- Certains routeurs utilisent néanmoins encore des access-lists pour bloquer le trafic non désiré. Ce type de filtrage sera progressivement retiré durant le marché. Seules les ACL permettant la protection des routeurs resteront à terme.

Le schéma ci-dessous illustre les chemins possibles pour les flux entre deux sites SIRes.



Chaque site dispose d'un routeur nominal et d'un routeur de secours

En mode nominal, les échanges entre sites passent par la connexion L3VPN fournie par RENATER. (Connexion à minima à 100Mb/s pour les délégations et 10Gb/s sur les centres serveurs de l'IN2P3 et d'Elancourt)

Le routeur nominal peut être relié à RENATER soit en direct soit au travers d'un réseau métropolitain ou de campus.

En cas de panne de la liaison nominale, les flux passent par un tunnel VPN IPSEC empruntant souvent un chemin différent du lien nominal et arrivant sur le lien de secours du second site.

Il y a aussi la possibilité de passer par un tunnel VPN chiffré partant du routeur de secours du premier site, utilisant l'accès ADSL ou fibre privé de celui-ci et arrivant sur le lien de secours du second.

La haute disponibilité est assurée par des mécanismes d'« AS prepend » et « communautés » BGP pour le distant et HSRP ou BGP pour le local.

Sur le site de la DSI Toulouse, un service de VPN pour utilisateurs nomades et de multiples tunnels ipsec vers les sites des sous-traitants exploitant les applications de la DSI sont en place, ceci permettant leur accessibilité au réseau Sires.

C'est sur le site de l'IN2P3 Villeurbanne que sont présents la plus grande partie des équipements du périmètre. L'ensemble du réseau local du site est administré par le titulaire du présent marché.

Les différents réseaux internes sont routés et filtrés par les firewalls.

3.16.3 Les équipements

Ils sont accédés par leur adresse d'administration privée.

Une description synthétique des équipements et modules actuellement en production est fournie en annexe.

Le nombre et le type de ces équipements peut être amené à évoluer tout au long du marché.

Les types d'équipements actuels sont essentiellement : routeurs, commutateurs, pare-feu

Il y a également sur les sites de la DSI : contrôleurs wifi, bornes wifi.

Ils peuvent être sous la forme d'appliances physiques ou virtuelles. Les modalités de gestion sécurisée des équipements sous forme virtuelle seront discutées lors de l'initialisation du marché.

4 PRÉSENTATION DU MARCHÉ ACTUEL

Le titulaire du marché actuel en cours d'exécution a en charge :

- La supervision du réseau.
- L'exploitation de celui-ci.
- Le suivi des alertes de sécurité et la mise à jour des équipements.
- La maintenance des matériels et des logiciels associés.
- Diverses prestations annexes.

4.1.1 Organisation

Un plan de service, mis en place en début de marché, définit l'organisation, les engagements réciproques, les indicateurs de qualité de service attendus, les procédures.

Un responsable opérationnel de compte et un ingénieur de suivi de compte locaux sont affectés (non exclusivement) à ce marché. Des rencontres mensuelles avec ceux-ci permettent un suivi de la qualité des prestations.

4.1.2 Supervision

Tous les équipements du périmètre sont supervisés soit par polling snmp V3 .

Les débits des interfaces, charges, erreurs de tous les équipements, gigue et latence des liens (entre autres) sont graphés.

Une vingtaine d'incidents sont traités par mois. (Panne électrique, coupure opérateur ...)

4.1.3 Exploitation

Les interventions en heures non ouvrées sont traitées par le « Network Operations Center » mutualisé du titulaire. Les interventions en heures ouvrées sont affectées à un des exploitants ou à l'ingénieur de suivi de compte.

Les demandes de modification des configurations sont faites soit directement par les délégations régionales (pour leurs routeurs propres) soit par les équipes réseau ou exploitation de la DSI au travers de l'outil ITSM du titulaire.

Sont traités actuellement environ 1000 tickets annuellement dont 30% pour des incidents et 70% pour des demandes de changement.

Dans les incidents, la plupart sont mineurs et souvent liés à des problèmes sur les liens ADSL. La part des incidents critiques est très faible (1 ou 2 par an) essentiellement pour des pannes électriques sur les centres serveurs.

Le comité de crise a été réuni une fois sur la durée du marché.

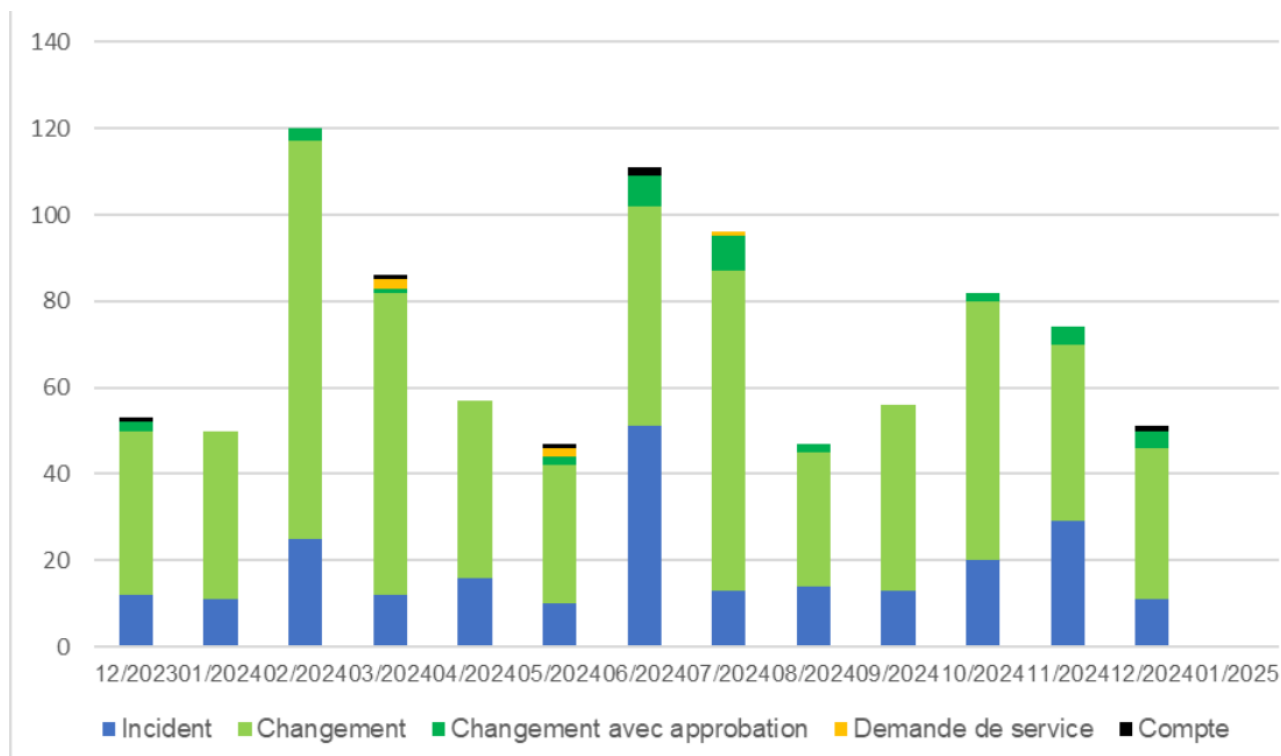
La plupart des changements (environ 90%) sont simples. Ils consistent essentiellement à la mise en place de filtres sur les routeurs ou les pare-feux des différents sites.

Des mises à jour sont réalisées régulièrement sur les équipements. Souvent en heures ouvrées en fin ou début de journée ou durant les arrêts de service (4 arrêts de service annuels).

Ces mises à jour sont en moyenne au nombre de 4 par an sur les équipements Palo Alto et 1 sur les équipements Cisco.

L'exploitant organise directement la mise à jour avec les sites impactés.

Évolution du nombre de tickets au cours de la dernière année



4.1.4 Suivi des alertes de sécurité

Les exploitants vérifient quotidiennement la présence d'alertes de sécurité (auprès d'un CERT et des constructeurs) impactant le parc.

S'il y a un impact, il fournit au CNRS une analyse précisant le degré de risque, les équipements impactés, les contournements possibles ou la nécessité d'une mise à jour logicielle.

En fonction de la criticité, les mises à jour sont appliquées par l'exploitant sous un délai qui peut aller de l'immédiateté à l'attente de l'un des quatre arrêts annuels du SI.

4.1.5 Maintenance

Dans le cadre des précédents marchés, on a observé qu'environ 2 équipements étaient remplacés annuellement.

5 DÉFINITION DU BESOIN DU CNRS POUR LE NOUVEAU MARCHÉ

5.1 GÉNÉRALITÉS

Le CNRS a une exigence de disponibilité et de qualité du service réseau liée à la criticité des applications hébergées sur les centres serveurs.

Les éléments capitaux de ce nouveau marché sont :

- La qualité du choix des indicateurs et le bon suivi des SLA.
- Une capacité à analyser rapidement une alerte de sécurité, la classer et définir et dérouler un plan d'action adapté.
- L'autonomie des équipes du prestataire afin de permettre un fonctionnement optimal du réseau en 24/24 7/7 sans intervention technique des équipes CNRS
- Une très bonne connaissance et une parfaite maîtrise de l'architecture de nos Centres serveurs et de SIREs, accompagnée d'une capacité à analyser un blocage ou à escalader dans des délais restreints.
- Un outillage de supervision/exploitation complet, rapide, simple et accessible par tous les intervenants avec des rôles dédiés. (DSI, Délégations, titulaire).

5.2 GOUVERNANCE DU MARCHÉ

5.2.1 Organisation

Le CNRS et le titulaire mettent en place les acteurs nécessaires pour assurer le bon fonctionnement et le pilotage du marché

5.2.1.1 Le Titulaire

Le CNRS laisse le Titulaire proposer l'organisation qu'il considère la plus adéquate pour répondre aux besoins du marché. La complexité de l'architecture et la criticité des applications nécessitent néanmoins la présence d'ingénieurs ayant une connaissance réelle et précise de SIREs ainsi que l'expérience et les compétences requises à l'administration de réseaux d'envergure équivalente.

Pour répondre à cette demande le titulaire devra mettre en place, dès le lancement du marché, une équipe restreinte et stable affectée à la prestation. Cette affectation n'est pas forcément exclusive.

Il décrit précisément sa composition et son fonctionnement (nombre, profils de compétences, organisation) afin d'atteindre l'objectif de niveau de service rendu.

L'ensemble des intervenants devront participer régulièrement et physiquement au comité opérationnel. Ils auront une maîtrise parfaite de la langue française.

Ils doivent pouvoir être impliqués, même en heures non ouvrées, dans la résolution d'incidents critiques ou majeurs. Les profils des intervenants sont fournis dans la réponse.

La majorité des équipements exploités nécessitent des compétences « Cisco » (commutateurs, routeurs, firewalls) et « Palo Alto » (firewalls), ceci n'étant pas exclusif. (du matériel d'autres fournisseurs pouvant être intégré).

Des firewalls checkpoint et stormshield vont par exemple être intégrés prochainement.

La description de l'équipe devra donc indiquer le niveau de compétences dans ces technologies, les moyens de formation dont ils disposent et le support qu'ils peuvent trouver au sein de leur entreprise.

5.2.1.2 Le CNRS

Coté CNRS, les intervenants sont :

- Le ou Les responsables contractuels qui ont en charge le suivi de la partie contractuelle du marché.
- Les membres de l'équipe Ingénierie et Expertise des infrastructures de la DSI ayant une compétence réseau (5 personnes). Ce seront les contacts principaux des équipes techniques du titulaire.
- L'équipe d'exploitation (composée à ce jour de 10 personnes)
- Les équipes SSI des délégations régionales qui sont amenées à faire des demandes de changements ou d'incidents.
- L'équipe cybersécurité de la DSI.

Les équipes en délégation sont généralement composées d'une dizaine de personnes. (Équipe SSI).

Elles gèrent leur réseau interne et sont souvent le contact pour joindre les réseaux de campus ou métropolitains.

Il n'y a pas forcément de personnel dédié uniquement au réseau.

Il faut considérer que leur seule action sur les équipements peut un geste de proximité guidé.

Elles sont dirigées par un responsable des systèmes d'information (RSI). Chaque site dispose également d'un responsable sécurité des systèmes d'information (RSSI). Cette fonction est néanmoins souvent dévolue au RSI.

Un document indiquant les contacts autorisés à émettre des demandes auprès du titulaire dans chaque site connecté est fourni au titulaire. Ce document est établi et mis à jour par la DSI sur information du RSI du site connecté.

5.2.2 Gouvernance

Il est nécessaire de définir entre le titulaire et le CNRS une structure de coordination impliquant des représentants de chaque organisation ayant des compétences dans les domaines traités.

Cette coordination, proposée par le CNRS distingue plusieurs niveaux :

- Le Comité de pilotage pour les aspects stratégiques et contractuels.
- Le Comité Opérationnel pour le suivi régulier des prestations.
- Le Comité de Suivi Cybersécurité pour le suivi des indicateurs et événements de sécurité
- Le Comité de gestion de crise.

5.2.2.1 Le comité de pilotage

Le Comité de pilotage est constitué de membres exerçant un pouvoir de décision : Il est consulté pour les décisions stratégiques ou les modifications d'orientation du marché ou tout changement dans le PAQ.

Il est constitué :

- du responsable de compte du titulaire
- du responsable sécurité du titulaire
- d'un représentant opérationnel de la DSI
- du Directeur des systèmes d'information de la DSI du CNRS ou de son représentant
- du RSSI de la DSI ou de son représentant.
- du Délégué Régional du CNRS en région Occitanie ouest, signataire du marché ou de son représentant

Il peut être réuni à la demande du CNRS pour valider les grandes étapes telles que le lancement du projet.

Le cas échéant, il intervient comme structure de recours et de négociation pour traiter les situations bloquantes qui n'ont pu être réglées en Comité Opérationnel... Le titulaire peut également solliciter une réunion extraordinaire de ce comité soit auprès du Directeur des systèmes d'information de la DSI du CNRS, soit auprès du Délégué Régional du CNRS en région Midi-Pyrénées.

Chaque réunion fait l'objet d'un compte rendu, rédigé par le titulaire et approuvé par les deux parties.

5.2.2.2 Le comité opérationnel

Le comité opérationnel est constitué au minimum par le responsable opérationnel de compte et par un des ingénieurs de suivi de compte du titulaire.

Au niveau du CNRS, le responsable contractuel et les ingénieurs de l'équipe IEI de la DSI en font partie.

Le comité se réunit au minimum une fois par mois dans les locaux de la DSI CNRS à Labège (31).

Les équipes du titulaire doivent préparer et envoyer préalablement à la réunion le tableau de bord mensuel sous forme électronique au plus tard 5 jours avant la réunion.

Celui-ci indique, entre autres :

- L'évolution des tickets d'incidents et de changement sur le mois et l'année en fonction du type d'incident et du lieu.
- Les charges en entrée et sortie des interfaces importantes, les taux de perte. (Graphes + tableau récapitulatif pour les interfaces d'entrée de site).
- L'évolution de la disponibilité des équipements et des liens supervisés sur le mois et l'année
- Tableau d'obsolescence du matériel.
- Tous les éléments qui sont apparus étonnant au titulaire (erreurs sur des interfaces, volumétrie trop importante, stabilité tables de routage, mauvaise qualité d'un lien (gigue, RTT...)).
- Un suivi des actions en cours.
- Les évolutions proposées par le titulaire.
- Une explication sur les tickets ayant posé problème.
- Les alertes de sécurité liées aux équipements exploités ou plus globalement aux problématiques de sécurité pouvant impacter l'ensemble des sites.

La présentation sous la forme de graphiques est à privilégier.

Ce document doit présenter les temps de réalisation des différentes prestations afin de pouvoir vérifier leur conformité avec les SLA.

Ces tableaux de bord sont finalisés lors de la phase de prise en main et peuvent évoluer tout au long du marché selon les besoins.

Sur la base du tableau de bord, les différents indicateurs sont analysés, l'état du réseau et les diverses actions entreprises ou à entreprendre sont évoquées.

Des intervenants externes (commerciaux, experts) peuvent être conviés par le titulaire ou par la DSI pour traiter un point du suivi du marché.

Chaque réunion fait l'objet d'un compte rendu, rédigé par le titulaire et approuvé par les deux parties.

5.2.2.3 Comité de suivi Cybersécurité (COSEC) - (MOE CNRS, titulaire)

Il a pour objet le pilotage des sujets relatifs à la sécurité des systèmes d'information (mise en place du PAS, revue du PAS, suivi des dérogations, suivi de l'avancement des actions de sécurité, mise en place des métriques de sécurité, suivi des métriques en indicateurs de sécurité, ...), bilan des faits marquants sécurité sur la période, revue des accès privilégiés, arbitrage des recommandations sécurité, revue de la PSSI et de sa mise en œuvre.

Il est composé pour le CNRS du responsable de la prestation, du correspondant à la sécurité des systèmes d'information, de membres des équipes projets en fonction de l'ordre du jour et pour le titulaire, à minima, du chef de projet et du correspondant sécurité des systèmes d'information.

Les comités sécurité se tiennent tous les 6 mois ou au besoin à l'initiative d'une des parties, en présentiel ou en visioconférence à défaut

Livrables associés à la charge du titulaire :

- Ordre du jour
- Convocations, documents d'organisation
- Comptes-rendus, soumis à validation du **CNRS**
- Plan d'assurance sécurité mis à jour
- Tout document demandé par le **CNRS** sous préavis de 8 jours avant la tenue des débats (liste non exhaustive)

Le **titulaire** fournit un tableau de bord et des indicateurs associés permettant d'évaluer le niveau de sécurité **au minimum** sur les thématiques suivantes :

- Gestion des incidents de sécurité
- Gestion des correctifs de sécurité (patch management)
- Gestion des vulnérabilités
- Gestion des traces
- Gestion des droits et personnels sur le projet
- Gestion des sauvegardes

5.2.2.4 Le comité de gestion de crise

Le comité de gestion de crise est réuni à la survenance d'un événement majeur (de cause interne ou externe). Il est constitué :

- Du responsable de compte du titulaire
- Du responsable sécurité du titulaire dans le cas de problèmes liés à la sécurité.
- Du responsable sécurité de la DSI du CNRS ou son représentant.
- Du DSI du CNRS ou son représentant.
- D'un représentant opérationnel de la DSI
- De tous les intervenants impliqués dans la résolution de l'incident.

Le comité est dissous à la disparition de l'événement qui a gouverné sa réunion, et en tout état de cause à l'initiative du CNRS.

Chaque réunion fait l'objet d'un compte rendu, rédigé par le titulaire et approuvé par les deux parties.

5.2.3 Documentation

5.2.3.1 Plan d'Assurance Qualité (PAQ)

Dans le cadre de la prestation de « Prise en charge », le titulaire fournit un plan d'assurance qualité (PAQ) qui traite :

- De l'objet du Plan Qualité (objectif et contenu ; positionnement dans le système qualité global, responsabilités associées au plan qualité ...),
- Du pilotage des prestations (organisation du marché, procédures de coordination et comités mis en place (fond documentaire, les outils pour traitement des anomalies et des incidents ...),
- Du plan de production (rappel des moyens matériels et logiciels nécessaires à la prestation et présentation du cadre méthodologique destiné à assurer la qualité du service du marché ...).
- Des processus de traitement des incidents et changements et des moyens de suivi par le CNRS.
- Du rôle de chaque profil d'intervenant.
- Des procédures d'escalade (avec les délais de traitement dans chaque étape).
- Des modalités de mise en place du comité de gestion de crise.
- Des rôles et responsabilité par type d'action (RACI).
- Des éléments figurants dans le tableau de bord mensuel de la prestation.
- Du plan de réversibilité (étapes, planning, responsabilités)

5.2.3.2 Plan d'assurance sécurité (PAS)

Dans le cadre de la prestation de « Prise en charge », le titulaire finalise un plan d'assurance sécurité (PAS) qu'il aura fourni dans sa réponse :

- Traite de l'objet du Plan Sécurité (objectifs et contenu, organisation du système de management de la Sécurité dans le déroulement du marché, la méthodologie associée, les responsabilités des différents acteurs...)
- Définit les processus d'évolution de ce PAS tout au long du marché et son applicabilité
- Déclina les exigences de sécurité spécifiées par le CNRS et applicable dans le cadre du marché.
- Sert de liens entre les différentes procédures organisationnelles et techniques et les exigences de sécurité du CNRS
- Décrit les différents sites sûrs du titulaire.

5.2.3.3 Fonds documentaire

Le titulaire produit et maintient, entre autres, l'ensemble des documents suivants :

- Référentiel des documentations
- La liste des équipements administrés, maintenus et supervisés avec le numéro de série et la version système installée.
- Les classes d'adresses des sites.
- Les Schémas des sites (Wan, Lan pour les centres serveurs) et les contacts campus/réseaux métropolitains.
- Liste des indicateurs par famille d'équipements.
- PAQ
- PAS

Le CNRS produit et maintient :

- La liste des interlocuteurs CNRS.

Le titulaire assurera la gestion des versions de l'ensemble des documents qui seront accessibles en permanence à l'équipe réseau de la DSI du CNRS.

Ils seront stockés sur le service de partage de fichiers du CNRS (sdrive).

Les documents seront au format MS Office (hors offre cloud) en version courante ou n-1 et seront fournis sur support électronique :

- MS Word, MS Excel, MS PowerPoint
- MS Visio pour les schémas

5.3 CARACTÉRISTIQUES DES PRESTATIONS TECHNIQUES ATTENDUES

5.3.1 Prestation de maintenance

Les équipements concernés par le marché étant répartis sur la France entière (dans les délégations Régionales du CNRS, le Siège, les 2 sites DSI et les centres serveurs), le titulaire possède une capacité d'intervention nationale avec des stocks de tous les équipements du marché permettant de répondre aux délais de rétablissement définis ci-après dans le CCTP. Ces stocks évoluent en fonction des équipements ajoutés ou supprimés de l'inventaire. Le stockage d'équipements de secours dans les armoires de production n'est pas prévu.

Tous les routeurs d'entrée de site sont maintenus par le titulaire.

Les équipements du réseau Local de certains sites sont ou seront également intégrés dans le marché (Les centres serveurs, Les sites DSI, le Siège, la délégation de Nice)

Le CNRS se réserve la possibilité d'inclure les réseaux locaux d'autres sites.

Lors du déclenchement d'une maintenance :

- L'équipement de remplacement doit être similaire à l'équipement en panne, de même marque et de modèle équivalent (fonctionnalités, performances, date de fin de vie) ou supérieur.
- Les équipements de remplacement ne sont pas nécessairement neufs, mais ils sont remis en configuration usine par le titulaire, avant paramétrage en conformité avec le matériel remplacé. Le Titulaire fournit impérativement un certificat d'authenticité du matériel, émis par le constructeur.
- La configuration sauvegardée précédemment doit être restaurée, les liaisons en place avant l'incident totalement rétablies et testées.
- Dans l'hypothèse où le Titulaire récupère l'équipement défaillant, il doit le remettre en configuration usine et fournir une attestation de cette opération au CNRS. Si le matériel est irrécupérable, il fournit une attestation de destruction.

En heures non ouvrées, le titulaire devra déclencher de sa propre initiative les actions de maintenance sur des incidents critiques ou majeurs. Il complète le ticket d'incident. La procédure d'information en temps réel du contact CNRS sera discutée durant les ateliers de lancement du marché.

À chaque référence d'équipement correspondra une UO de maintenance. Le coût de cette UO sera fonction de la plage de prix public d'achat avant remise et du niveau de maintenance désirés.

Le prix public prend en compte les modules, cartes d'extension, alimentations et autres éléments en place dans l'équipement. La maintenance englobe donc également ces dispositifs.

Pendant la durée d'exécution du marché, le CNRS se réserve la possibilité de se substituer au Titulaire en ce qui concerne la réassurance auprès du fabricant du matériel. Ce serait en particulier le cas dans l'hypothèse où le CNRS conclurait un marché global avec un ou des constructeurs.

Ainsi, en cours de marché, des équipements pourront basculer d'un mode de maintenance à l'autre à chaque échéance annuelle, avec une prévenance minimale de trois mois de la part du CNRS.

Dans ce but des UO de « support à la maintenance » sont prévus.

Dans ce cadre, l'exploitant gère le remplacement de l'équipement avec le mainteneur désigné. Suite à la réception de l'équipement sur site, il devra intervenir physiquement pour remplacer le matériel, le mettre à jour, remettre en place la configuration puis tester les liens jusqu'à retour à l'état nominal. Le Titulaire efface la configuration propre au CNRS de l'équipement remplacé et remet le matériel en configuration usine. Dans l'hypothèse où cette opération est techniquement impossible, il en informe sans délai le CNRS, afin de lui permettre de prendre les mesures adéquates. L'exploitant devra également suivre le cycle de renouvellement des maintenances comme il le fait pour les autres matériels afin de prévenir en amont le CNRS de la nécessité de se réassurer.

5.3.1.1 Support logiciel

Lorsque le Titulaire assure la maintenance des matériels, il prend en charge auprès du constructeur les coûts liés au support des fonctionnalités logicielles système (OS) permettant la mise à jour des versions actives sur les équipements.

Lorsque le Titulaire n'assure qu'un « support à la maintenance », il s'appuie sur le contrat conclu par le CNRS auprès du constructeur pour obtenir et implémenter les mises à jour des versions actives sur les équipements. Le Titulaire gère le contact avec le constructeur. En cas de difficulté, il en informe sans délai le CNRS.

➤ **Résultat attendu**

Un remplacement dans les délais définis dans le contrat de service (cf. 7.4.4)

5.3.2 Prestation de supervision et traitement des incidents

L'objectif de cette prestation est d'assurer une surveillance des équipements du périmètre afin de détecter toute panne impactant le bon fonctionnement du réseau et de déclencher les actions correctives en 24/24 7/7 selon le niveau de service attendu.

Les indicateurs issus des collecteurs, permettant la surveillance, sont collectés en temps réel, et un historique sur la durée du marché est disponible.

Le titulaire devra indiquer précisément l'architecture permettant la supervision depuis son/ses sites. (Redondance des équipements, des liens...).

Une solution via des liens dédiés est à privilégier.

Il doit dimensionner ses liens pour permettre une supervision efficace mais également l'administration quotidienne. (En particulier l'envoi d'images système vers les équipements dans un délai restreint).

5.3.2.1 Détection des pannes / problèmes

Cette supervision doit permettre la détection rapide des pannes tant au niveau hardware, software (routage) qu'au niveau de l'état des liaisons.

Elle doit s'intéresser (en fonction des équipements) a minima à :

- L'état des peerings bgp.
- Le nombre de préfixes reçus / envoyés. (Avec alerte sur changement significatif)
- La liaison utilisée pour atteindre les centres serveurs depuis les délégations et inversement (nominale, secours, secours via opérateur privé)
- L'état des tunnels VPN sites à sites.
- L'état des accès « out of band » aux équipements des Datacenters.
- La température, l'état des ventilateurs.
- L'alimentation pour les équipements redondés électriquement.
- L'accessibilité des interfaces d'administration des différents équipements.
- L'état des ports (un ensemble de ports à surveiller est fourni à l'exploitant).
- Les débits inhabituels sur ces ports
- Gigue, erreurs et temps de réponse moyen entre les Délégations régionales et les Centres serveurs.

Une vérification proactive de certains éléments de configuration sera à réaliser régulièrement pour vérifier l'homogénéité du parc (utilisation de playbooks ansible à privilégier).

Tous les indicateurs sont définis durant la phase de lancement et peuvent évoluer durant la durée du marché.

La génération de traps SNMP depuis les équipements est privilégiée pour permettre une détection rapide des pannes.

Quelques sondes pourront être mises en place par le CNRS durant le marché pour tester l'état des liaisons intra-site. Les valeurs retournées par celles-ci devront également être monitorées.

5.3.2.2 Affectation des incidents

Les incidents sont catégorisés en :

- **Incident critique**

L'incident provoque une indisponibilité totale d'un site sensible (centres serveurs, sites DSI, siège du CNRS) ou des applications nationales du SI. Il peut également être déclenché à la suite d'un incident de sécurité majeur ou critique.

- **Incident majeur**

L'incident provoque un fonctionnement dégradé d'un site sensible (passage par un lien de secours par exemple). L'accès aux applications nationales est néanmoins possible.

Il peut également provoquer l'indisponibilité totale d'un site non-sensible.

- **Incident mineur**

Un événement sans impact ou avec un impact faible sur la qualité de service rendue par le réseau.

La classification des niveaux d'incident est proposée par le titulaire lors de la déclaration. Le CNRS est en droit de requalifier le niveau d'incident à la hausse ou à la baisse. Le titulaire traite alors l'incident selon les modalités associées à ce niveau.

5.3.2.3 Traitement d'un incident

Un ticket est généré dès qu'une anomalie est détectée (maximum 15 minutes après sa survenance) ou signalée via le guichet unique. Différentes procédures seront mises en œuvre pour être en adéquation avec la sévérité de l'incident.

L'équipe réseau CNRS et les personnes habilitées du site impacté doivent être informés **régulièrement** (a minima toutes les demi-heures en cas d'incident critique, toutes les heures en cas d'incident majeur) de l'évolution du ticket et des différentes actions mises en œuvre.

Une procédure d'escalade rapide est prévue afin de ne pas rester dans un mode de diagnostic de premier et second niveau plus :

- De huit heures ouvrées pour un incident mineur.
- De deux heures H24 7/7 maximum pour un incident majeur
- D'une heure H24 7/7 maximum pour un incident critique

Elle implique un service d'expertise au niveau du titulaire et permet de :

- Résoudre l'incident et corriger les anomalies (modification de configuration) sur le/les équipements.
- Déclencher une mise en sécurité du système.
- Déclencher une action de maintenance
- Solliciter un tiers : opérateur.
- Remonter directement au constructeur. Lorsque le CNRS a conclu le contrat de support avec le constructeur, le Titulaire agit au nom et pour le compte du CNRS. En cas de difficulté, il en informe le CNRS sans délai.

Dans ce cas il adapte le niveau de priorité chez le constructeur au niveau de l'incident.

Par ex : Sur un incident critique le titulaire ouvre un ticket de priorité 1 chez le constructeur.

Lorsque le Titulaire conclut les contrats de support, la capacité à créer directement un ticket chez les constructeurs du marché est importante pour le CNRS. Lorsque le CNRS a conclu lui-même le contrat de support, cette responsabilité lui incombe.

Merci d'indiquer cette capacité pour le constructeur Cisco.

Le titulaire fournit le contenu des procédures d'escalade qu'il applique en indiquant le temps maximum affecté à chaque étape afin de répondre aux délais de résolution indiqués dans la définition des prestations.

Le déclenchement d'une maintenance ou de l'intervention d'un tiers allonge le délai de résolution :

- de la durée de GTR liée à l'équipement.
- du temps de la GTR liée à la liaison du tiers contacté
- du temps d'intervention du tiers si aucune GTR n'est associée à son action.

Dans le cas d'un incident critique, le titulaire privilégiera toujours les solutions limitant le délai d'indisponibilité quitte à être pour un certain temps dans un mode « non optimal » (par exemple sans redondance).

5.3.2.4 Gestion des tiers

Le titulaire assure le suivi des intervenants (exploitant, opérateur, équipe de maintenance, campus, réseau métropolitain ...) dont il sollicite l'intervention. Ce suivi permet de tracer les actions en cours et de suivre l'état d'avancement de la résolution des incidents.

Il peut être amené, par exemple, à contacter et faire intervenir le titulaire du marché d'hébergement et RENATER (liens WAN des centres serveurs), le prestataire fournissant les liens de secours (ADSL ou Fibre) ou encore les sous-traitants ayant une terminaison VPN sur les routeurs d'un centre serveur.

Le titulaire relance régulièrement le tiers et prévient le CNRS du défaut d'un intervenant dans ces engagements de temps de rétablissement afin de ne pas rester dans un mode « gelé ».

La défaillance d'un tiers ne dégage pas le titulaire de ses obligations, à moins qu'il ne démontre avoir conduit toutes les diligences nécessaires et informé le CNRS des difficultés rencontrées, afin de lui permettre de prendre les mesures utiles.

5.3.2.5 Clôture de l'incident

Toute anomalie ou incident résolu fait l'objet d'une clôture dans la base de gestion des tickets et incidents et est commenté dans le tableau de bord mensuel.

L'ensemble des données relatives aux pannes survenues sur le réseau est stocké durant toute la durée du marché (Numéro de ticket, cause, actions entreprises, impact sur le réseau).

A chaque groupe de matériel (défini sur la base de la complexité de l'équipement) est associé un coût unitaire mensuel. La réponse se fera sur la base des groupes définis dans le tableau des équipements. Le positionnement d'un nouvel équipement dans les différents groupes sera discuté lors des comités opérationnels.

➤ Résultat attendu sur la partie « incidents »

Le CNRS attend une remontée exhaustive des anomalies et incidents, une durée maximale annuelle d'indisponibilité de 8 heures de l'outillage de supervision et un traitement dans les SLA des différents incidents. Cet outillage est fourni et administré par le titulaire.

Si ces équipements de supervision doivent être placés sur le réseau du CNRS, ceux-ci sont de préférence situés dans le centre serveur (IN2P3). Dans le cas contraire, la volumétrie des échanges doit être limitée pour ne pas pénaliser les flux utilisateurs.

Le CNRS attend également un suivi précis des tickets d'incidents ouverts et une résolution des incidents dans les délais prévus.

5.3.2.6 Mise en place et administration d'un système permettant de générer des graphes.

Le titulaire fournit et héberge un système de graphes permettant de suivre l'évolution en temps réel de divers indicateurs de chaque équipement.

Il permettra d'accéder à un historique sur la durée totale du marché.

Cela inclut à minima :

- Charge CPU
- Charge mémoire
- Débit de toutes les interfaces
- Erreurs sur toutes les interfaces
- Gigue, latence, erreurs sur les liaisons WAN entre le site et les centres serveurs
(IP SLA disponible sur les routeurs)

Tous les autres indicateurs seront définis durant la phase de lancement.

➤ **Résultat attendu sur la partie graphes**

- Avoir des graphes accessibles rapidement par la DSI et les Délégations régionales (limité à leurs routeurs).
- Pouvoir zoomer sur une période réduite (heure). Pour cela, l'intervalle de prise d'information sur les équipements doit être assez réduit (max 5 minutes).
- Permettre un accès à ces données sur la durée du marché.

5.3.3 Prestation d'exploitation

L'objectif de cette prestation est de réaliser les actions quotidiennes permettant le bon fonctionnement du réseau. Le titulaire précise l'architecture technique permettant l'exploitation depuis son/ses sites.

5.3.3.1 Gestion des configurations

L'objectif de cette prestation est de disposer de la dernière configuration des équipements en cas de panne ainsi que d'une version de cette configuration avant et après chaque modification. Elle doit également permettre de comparer des configurations à diverses dates du marché.

5.3.3.2 Sauvegarde des configurations.

Le titulaire met en place un système automatisé de sauvegarde des configurations de tous les équipements du périmètre. Le titulaire et le CNRS ont à disposition l'ensemble des fichiers de configuration complets avant et après chaque modification.

Les configurations sont à conserver jusqu'à la fin du marché et à détruire sur demande du CNRS, il sera alors fourni au CNRS une attestation de destruction.

Une attention particulière est portée par le CNRS sur l'accès et le stockage de ces sauvegardes (pérennité, sécurisation d'accès, localisation des données). Le titulaire a décrit dans son offre l'outillage et la politique de sauvegarde en place.

À tout instant, le CNRS peut récupérer les différentes versions des sauvegardes.

Des informations sur chaque version (date, auteur, contenu et cause du changement...) sont également stockées.

Le titulaire fournira au CNRS une fois par an le résultat d'un test de comparaison entre la totalité des données présentes sur les sites de production et ces mêmes données issues d'une sauvegarde.

Il devra tester annuellement la remise en place d'une sauvegarde sur un échantillon de chaque type de matériels et fournir un compte rendu de cette action.

5.3.3.3 Affichage de configurations.

Les équipes SSI ont accès à la configuration de leurs équipements (hors mots de passe) et la DSI à toutes les configurations.

L'accès aux configurations doit être **rapide**, fiable, sécurisé et permettre une comparaison entre deux versions.

Il est également possible d'afficher un suivi des modifications par équipement, de connaître la date, l'auteur et le contenu de la modification.

5.3.3.4 Politique de gestion des logs.

Le titulaire met en œuvre un ou des dispositif(s) de collecte, stockage et scellement des journaux d'événements émis par les équipements dont il a la responsabilité opérationnelle. Il collecte sur ces équipements les événements permettant au CNRS d'assurer, sur requête judiciaire, la communication aux autorités de l'activité des usagers des SI qui ont été accédés au travers de ces équipements.

Outre les logs purement système et ceux de refus générés par les ACLs, le titulaire collecte également les flux légitimes traversant les routeurs des différents sites (netflow ou ACL en permit).

La DSI du CNRS doit avoir accès en lecture à ces logs.

Le titulaire s'assure par tout moyen de la conservation **intègre et disponible** de ces données pendant une durée de 12 mois glissante, conformément à la réglementation (art L.34-1 du code des postes et des communications électroniques, loi informatiques et libertés 78-17 du 6 janvier 1978).

Le titulaire indique où et comment sont stockés et sécurisés ces logs.

Résultat attendu

- Un système de collecte, stockage, et scellement des journaux d'événements conforme à la réglementation
- La description des modalités de la garantie d'intégrité et de disponibilité de ces données pendant la durée légale
- La description d'une procédure d'accès à ce système sur requête judiciaire

5.3.3.5 Gestion des changements

Ces modifications peuvent être très variées et touchent toute la configuration des équipements.

La plus grande partie des demandes concerne néanmoins des modifications de filtrage.

Le titulaire doit appliquer les changements demandés par la DSI et les équipes SSI de délégation selon la liste des autorisations qui sera communiquée et mise à jour par la DSI.

Cependant, la DSI peut demander des modifications de routage sur n'importe quel routeur ce qui n'est pas le cas pour les équipes SSI.

Les droits de chacun sont définis lors de la mise en place du marché.

Les demandes de changement doivent avoir des niveaux de priorité définis par les demandeurs afin que le titulaire puisse organiser ses actions.

Dans tous les cas, les demandes de changement « simples » sont réalisées en moins de 4h ouvrées à partir de l'ouverture du ticket de changement. Celui-ci est ouvert au maximum 15 minutes après réception du mail de demande de changement.

Les actions sur les centres serveur sont toujours prioritaires sur des actions sur les routeurs de délégation.

Les demandes sont faites par mail sur une adresse unique ou via le système automatisé de gestion de tickets de la DSI du CNRS.

Les modifications sur plusieurs équipements devront de préférence être automatisées au travers de « playbooks » ansible partagés avec les équipes de la DSI.

Si cette automatisation n'est pas possible en début de marché, elle devra être mise en place au cours de celui-ci car importante pour la DSI du CNRS.

Une demande provenant du CNRS peut regrouper plusieurs actions

On définit trois types de changements afin de pouvoir en suivre les SLA:

Les **changements simples** : changement d'une ou plusieurs règles correspondant à une même fonction sur un équipement.

Les **changements medium** : changement d'une ou plusieurs règles correspondant à des fonctions différentes sur un ou deux équipements.

Les **changements complexes** : changements d'une ou plusieurs règles sur plus de deux équipements.

La durée de réalisation d'une demande est indiquée dans la définition de prestations (cf. §7.6.4 ci-dessous)

Les demandes peuvent être définies comme « urgentes » dans une limite de 25%.

La durée des changements complexes est discutée au moment de la demande mais ne doit pas excéder 24h.

Certains changements liés à des tests ou des évolutions nécessitant une coordination avec d'autres équipes peuvent nécessiter la présence téléphonique d'un intervenant du titulaire afin d'effectuer des modifications et des retours arrière. Ce type de changement sera réalisé en heures ouvrées (sauf achat de l'unité d'œuvre « extension horaire ») et la demande sera faite à minima un jour avant l'intervention. Un ticket unique résumant les différentes opérations à réaliser sera généré.

Des changements sur les équipements des sites de la DSI de Toulouse et des centres serveurs de l'IN2P3 peuvent être réalisés par l'équipe réseau de la DSI. Elle est responsable des incidents qui pourraient être engendrés par ces modifications.

L'équipe réseau de la DSI a également un accès total à tous les autres équipements. Mais la possibilité de modification directe n'est utilisée qu'en cas d'une urgence sécurité nécessitant une réactivité immédiate.

La DSI s'engage alors à prévenir le prestataire de l'action réalisée et de son contenu, de son étendue.

L'équipe réseau du CNRS est en copie de toutes les demandes et à la possibilité de suivre le traitement de ces demandes.

L'administration sera réalisée au travers du bastion de la DSI CNRS (Cyberark) avec un accès direct aux équipements en mode « brise-glace ». Celui-ci n'étant utilisé qu'en cas de non disponibilité du bastion.

➤ **Résultat attendu**

- Une simplification maximale des demandes et une utilisation, quand cela est possible, du formalisme déjà en place au CNRS.
- Des délais de réalisation respectueux des SLA

5.3.3.6 Support aux changements

Les demandeurs ont des connaissances en réseau très variables. Il se peut donc que les demandes ne soient pas précises ou mal explicitées. Il est du ressort du titulaire de contacter le demandeur afin de préciser avec lui la demande jusqu'à ce qu'elle soit réalisable.

Le titulaire doit alerter la DSI du CNRS si une demande est manifestement disproportionnée, risquée ou engendrant un risque sécuritaire important. Ces conditions seront abordées lors des ateliers de lancement du marché.

De plus, il doit mettre en œuvre les moyens pour participer activement à la réalisation du changement. Il pourra par exemple utiliser le système de stockage des logs décrit précédemment pour participer à l'analyse d'une erreur dans la demande.

➤ **Résultat attendu**

Une autonomie du titulaire qui peut suivre la demande de changement jusqu'à ce qu'elle soit totalement effective.

5.3.3.7 Gestion des versions système

Le titulaire est responsable de la mise à jour des versions logicielles des équipements et des services associés (VPN, signatures de menaces...).

Le titulaire doit consigner l'état des versions de tous les équipements et suivre les alertes de sécurité du CERT-Renater, du CERT-FR et des constructeurs des équipements afin de proposer au CNRS des évolutions de version qui lui semblent nécessaires.

Il suivra la procédure définie au §6.2.5 (Maintenance des systèmes – Gestion des vulnérabilités techniques) en cas d'alerte.

Le CNRS peut néanmoins demander ponctuellement une mise à jour logicielle spécifique soit pour l'ajout d'une fonctionnalité, soit en cas de problème sur une version. (Sur un ou tous les équipements).

Un changement de version est équivalent en termes de SLA à un changement complexe du paragraphe §5.3.3.5 ou à un incident critique du paragraphe §5.3.2.2 dans le cas d'une faille de sécurité nécessitant un upgrade urgent.

Dans ce cadre-là, sera décompté autant de ticket de changements que d'équipements mis à jour.

Les mises à jour des équipements devront être automatisées au travers de « playbooks » ansible partagés avec les équipes de la DSI.

➤ **Résultat attendu**

Des équipements à jour en termes de correction de vulnérabilité de sécurité et une vision à jour des versions en place dans le parc.

Un carnet de 100 changements mensuels correspond à l'unité d'œuvre de l'ensemble de cette prestation.
La nature des changements et le type de matériel sur lesquels ils sont appliqués ne sont pas différenciés.

5.4 OUTILLAGE

5.4.1 Guichet unique

Le titulaire doit offrir un point d'accès commun aux différents utilisateurs CNRS permettant de prévenir d'un problème impactant le réseau, s'informer sur l'état d'une demande ou sur un problème d'accès.

- **Mise en place d'un numéro téléphonique de contact**

Le titulaire fournit un service d'accueil téléphonique à tarification locale disponible en 24/7/365 permettant aux équipes de la DSI et aux personnels référencés des délégations de déclencher l'ouverture d'un ticket ou de suivre un ticket ouvert.

Ce numéro est de préférence réservé aux appels concernant le réseau SIREs. S'il est mutualisé, une référence simple doit permettre au personnel du titulaire de faire le rapprochement avec le réseau SIREs. Le numéro de la délégation permet à l'exploitant de repérer l'équipement concerné.

- **Mise en place d'une adresse mail.**

Comme pour le numéro téléphonique, ce mail permet de déclencher l'ouverture d'un ticket, de suivre un ticket. Il permet en plus de faire une demande de changement.

Les tickets doivent être créés et suivis dans l'outil « JIRA » du CNRS.

5.4.2 Portail de suivi

Le titulaire fournit un accès unique (de préférence) et rapide aux différents outils fournis par le titulaire pour réaliser les prestations précédentes.

- **Un accès Web sécurisé aux :**
 - Différents graphes (météo du réseau, charge des interfaces....)
 - Configurations des équipements
 - A des informations à destination des équipes de délégation, pouvant être modifiées par l'équipe réseau du CNRS. (Formalisme des demandes, fichiers ...)
 - Logs et flows

Le portail ou à défaut, les différents services doivent pouvoir être accédés avec des droits et vues différentes en fonction des utilisateurs (Les Délégations par exemple ne doivent pouvoir accéder qu'aux configurations/logs de leur équipement).

L'accès se faisant si possible avec une authentification unifiée et multi-facteurs.

Le CNRS disposant d'un service d'authentification centralisé (Janus) basé sur le gestionnaire d'identité Shibboleth (SAML2), il serait souhaitable que celui-ci soit utilisé dans le cadre de ces divers accès.

Une procédure « bris de glace » devra être mise en place en cas de problème sur ce module.

Ces aspects seront discutés lors des ateliers de lancement du marché.

6 EXIGENCES DE SÉCURITÉ

6.1 PRINCIPES GÉNÉRAUX

Concernant les aspects sécurité, le CNRS applique les principes généraux suivants :

- La Politique de Sécurité du Système d'Information (PSSI) du CNRS est arrêtée par la Direction du CNRS sur proposition du fonctionnaire de sécurité de défense (FSD),
- La Sécurité des Systèmes d'Information (SSI) repose notamment sur l'utilisation de techniques comme l'authentification des utilisateurs, le contrôle d'accès aux ressources, la non-répudiation, l'audit des traces de sécurité, etc. (cette liste est non exhaustive)

Chaque site est responsable de sa Politique de Sécurité, en accord avec la politique nationale, et met en œuvre les moyens qu'il juge nécessaires Firewall, réseaux privés virtuels (VPN), etc.).

6.2 MESURES DE SÉCURITÉ

Les paragraphes suivants explicitent et complètent le corps de doctrine de la PSSI du CNRS. Le titulaire décline ces mesures dans la partie sécurité de PAQ.

6.2.1 Gestion de la Sécurité par le titulaire

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

6.2.2 Sécurité du matériel

6.2.2.1 Travail dans les zones sécurisées

Le titulaire ne doit jamais intervenir physiquement sur un site du CNRS ou géré par le CNRS sans être mandaté et surveillé par du personnel du CNRS ou mandaté par le CNRS.

Il doit refuser d'assurer sa prestation, si le personnel encadrant du CNRS ou mandaté par le CNRS ne respecte pas son obligation de surveillance. Il notifie immédiatement ce refus à l'équipe réseau de la DSI. Le délai d'exécution de la prestation est suspendu jusqu'à ce que le personnel encadrant du CNRS ait pris les mesures nécessaires à cette surveillance.

Le titulaire n'est pas autorisé, sauf autorisation expresse du CNRS, à photographier, à faire des enregistrements audio ou vidéo des locaux ou des équipements du CNRS.

De même, il est interdit au titulaire d'introduire du matériel photographique, vidéo, audio ou d'autres matériels d'enregistrement dans les locaux du CNRS ou géré par le CNRS, sauf autorisation expresse du CNRS.

6.2.2.2 Sécurité du câblage

Le titulaire applique les directives du CNRS en termes de câblage des équipements. Notamment en ce qui concerne :

- le passage des câbles dans les cheminements prévus, si spécifié
- la séparation des câbles électriques et des câbles d'alimentation pour éviter les interférences
- l'utilisation du marquage spécifié et conforme aux standards, documentations et procédures du CNRS

Lors des opérations physiques sur les équipements, le titulaire assiste le CNRS :

- en relevant les erreurs de schéma de câblage sur la documentation
- en relevant les erreurs de câblage dans le choix des catégories de câble (cuivre ou fibre optique)
- en relevant des branchements d'équipements non-conformes

De même, le titulaire s'engage à ne pas prendre d'initiative sur le câblage des équipements du CNRS.

6.2.3 Gestion de l'exploitation

6.2.3.1 Gestion des modifications

Toute modification sur les systèmes doit entrer dans un processus de gestion des modifications.

Dans ce cadre, toute modification doit être :

- consignée par le titulaire
- si nécessaire, planifiée par le titulaire avec le CNRS
- évaluée par le titulaire pour anticiper les impacts, y compris sur la Sécurité afin d'avertir le CNRS en cas de risque ressenti.
- acceptée, pour les changements conséquents, par le CNRS
- transmise systématiquement, au moins pour information, au CNRS

Dans la mise en œuvre des modifications, le titulaire doit systématiquement prévoir des dispositifs de repli en cas d'échec des changements ou d'évènements imprévus.

Le titulaire n'apporte des modifications aux systèmes qu'après accord du CNRS sauf pour résoudre un incident critique ou majeur en heures non ouvrées.

Il est défini dans la phase de prise en charge le processus de gestion des modifications.

6.2.3.2 Acceptation du système

Toute modification conséquente des systèmes par le titulaire dans le cadre des prestations, doit être validée par un processus formel avec le CNRS avant toute mise en production. Ceci afin de valider que les exigences de matières de sécurité sont satisfaites.

6.2.3.3 Journal des opérations

Le titulaire doit journaliser les différentes actions et activités de ses intervenants sur les systèmes. Il conserve les traces de ces activités pendant une durée de douze mois glissants.

Ces journaux doivent au moins inclure :

- La date et l'heure à laquelle un évènement est survenu (succès ou échec)
- les informations relatives à l'évènement ou à la défaillance
- l'identification de l'opérateur concerné
- les actifs concernés

Le titulaire tient à disposition du CNRS ce journal des opérations, à la demande et sous 4 heures.

6.2.3.4 Journaux d'audit

Le titulaire met en place sur les systèmes la gestion des rapports d'audit dans le but d'enregistrer les activités des exploitants, les exceptions et les événements liés à la sécurité.

Ces traces sont archivées pour une durée de douze mois glissants, donc effacées au terme de leur durée de conservation. Ces journaux d'audit contiennent au moins les informations suivantes :

- les identifiants utilisateurs
- la date, l'heure et les détails relatifs aux événements significatifs
- l'identification du terminal de connexion (adresse IP)
- l'état des tentatives d'accès, réussies et avortées

Et si possible :

- les modifications apportées à la configuration du système
- l'utilisation des privilèges
- les adresses et les protocoles réseau

Ces traces sont déclarées au délégué à la protection des données du CNRS.

Les rapports d'anomalies ou de défaut sont activés et journalisés par le titulaire, sur les équipements dont la surveillance est à la charge du titulaire.

Il est défini entre le titulaire et le CNRS la liste exhaustive des rapports de défaut à gérer par les systèmes lors de la phase de prise en charge du marché.

Par la suite, le titulaire analyse régulièrement ces rapports de défaut. La fréquence d'analyse sera conforme aux niveaux de service défini dans le marché.

Ces rapports sont archivés pour une durée de douze mois glissants, donc effacés au terme de leur durée de conservation.

6.2.3.5 Protection des informations journalisées

L'ensemble des journaux d'événements collectés au cours de la prestation doivent être protégées contre l'effacement, la compromission et la divulgation.

Pour cela, le titulaire met en œuvre un système centralisé et sécurisé de gestion de ces traces et ouvre ce système au CNRS.

6.2.3.6 Surveillance de l'exploitation des systèmes

A tout instant, le CNRS se réserve le droit de surveiller en temps réel ou à posteriori les activités du titulaire sur les équipements du CNRS.

Cette surveillance est faite par le contrôle des journaux d'audit des équipements et la création de rapport automatique à partir du système centralisé .

6.2.3.7 Synchronisation des horloges

Le titulaire doit s'assurer que les horloges des systèmes du CNRS sont toujours synchronisées sur au moins deux sources de temps fiables, la même pour tous les équipements dont il a la gestion pour le CNRS.

Il doit également s'assurer que les horloges de ses propres systèmes sont également synchronisées sur au moins deux sources de temps fiables.

Il doit également veiller à éliminer les variations et les biais horaires, ou, le cas échéant, les documenter.

6.2.4 Contrôle d'accès

6.2.4.1 Politique de contrôle d'accès

Lors de la phase de prise en charge, il est établi conjointement avec le titulaire les politiques et matrices d'accès aux équipements et aux documents du CNRS. Cette politique définit aussi bien les accès logiques que les accès physiques.

L'objectif est de définir :

- des profils d'accès normalisés
- la gestion des droits en fonction de ses profils
- Le cloisonnement des rôles concernant le processus de contrôle d'accès (demande d'accès, autorisation d'accès et administration d'accès)
- Le processus d'autorisation formelle du contrôle d'accès
- Le processus d'annulation des droits d'accès

Dans le cadre des prestations, il est de la responsabilité du titulaire de maintenir à jour et de tenir à disposition les matrices nominatives d'accès des personnes clairement identifiées.

6.2.4.2 Passerelle sécurisée

Le CNRS est en cours d'extension de sa passerelle sécurisée (bastion d'administration) aux équipements réseau.

Le CNRS mettra en œuvre ce type de dispositif au lancement du marché ou durant la période d'exécution de celui-ci. Il sera mis en place avec le titulaire les procédures pour que les connexions et le contrôle d'accès vers les équipements du CNRS depuis les équipements du titulaire passent obligatoirement par ce dispositif.

La mise en place d'une telle passerelle permet au CNRS :

- d'authentifier la machine distante et la personne en charge du support
- de prévenir l'exploitation de vulnérabilités ou de portes dérobées sur le dispositif de télémaintenance
- de garantir la confidentialité et l'intégrité des données sur le SI
- d'assurer une traçabilité de confiance des actions effectuées par l'exploitant du centre de support
- de garantir l'innocuité de la fonction de télémaintenance vis-à-vis du système faisant l'objet du télédiagnostic ainsi que des systèmes connexes
- de garantir l'absence de fuite d'informations vers l'extérieur

Une procédure de type « bris de glace » sera mise en place pour palier à un problème sur cet outillage.

6.2.5 Maintenance des systèmes – Gestion des vulnérabilités techniques

Dans le cadre de la surveillance des systèmes du CNRS, le titulaire doit avertir le CNRS (responsable sécurité et équipe réseau) dès que des failles de sécurité concernant un type d'équipement du marché sont publiées (CERT-Renater, CERT-FR, constructeurs, etc.).

Les analyses d'impact, leur synthèse et l'éventuel plan d'action associé (application du correctif, modification de configuration, etc.) doivent être communiqués au CNRS, selon la notation CVSS v4.0 si disponible (sinon CVSS 3), dans les

- 1 heure 24/24 7/7 après parution de l'alerte pour des CVSS-B ≥ 9
- 4 heures ouvrées après parution de l'alerte pour des $9 > \text{CVSS-B} \geq 7$
- 10 heures ouvrées après parution de l'alerte pour des CVSS-B < 7

Au-delà de la simple analyse de correspondance entre une CVE et le parc en place, une analyse approfondie du type de risque (escalade de droits, DDOS...), des mitigations liées au positionnement de l'équipement ou encore des solutions de contournement disponibles est nécessaire,

Un outillage permettant d'automatiser cette analyse / mitigation des vulnérabilités serait un plus. Expliquer son fonctionnement s'il existe.

L'objectif étant de définir la nécessité réelle et l'urgence d'une action corrective.

La méthode d'avertissement du CNRS pour des incidents critiques sera discutée lors de la phase de lancement.

Suivant l'urgence de l'action corrective, celle-ci est appliquée en gestion des changements, soit en gestion des incidents (pour une faille avérée majeure ou critique cf. : « 5.3.2.2 Affectation des incidents ») sur décision du CNRS.

6.3 CLAUSES DE SÉCURITÉ

6.3.1 Obligations du titulaire

Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage à informer le CNRS des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le titulaire informe préalablement le CNRS de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le titulaire est responsable du maintien en condition de sécurité des systèmes de son périmètre pendant toute la durée des prestations.

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

6.3.2 Localisation des données

Les lieux d'hébergement des données du CNRS, dont les journaux et les sauvegardes de configuration satisfont aux exigences de sécurité du donneur d'ordres (CNRS). En l'occurrence, l'ensemble des données nécessaires à la réalisation des prestations sont stockées et traitées conformément à la Politique de sécurité des systèmes d'information de l'État.

Le titulaire communique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

6.3.3 Engagement de confidentialité

Les supports informatiques et documents fournis par le CNRS au TITULAIRE restent la propriété du CNRS.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont LE TITULAIRE prend connaissance à l'occasion de l'exécution du présent marché.

Conformément à l'article 34 de la loi informatique et libertés modifiée, LE TITULAIRE s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le titulaire s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

A ce titre, LE TITULAIRE ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable du CNRS. Le CNRS se réserve le droit de procéder ou faire procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par LE TITULAIRE.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut être également engagée sur la base des dispositions des articles 226-17 et 226-22 du nouveau code pénal

Le CNRS pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

6.3.4 Audits de sécurité

Le CNRS pourra, à tout moment, contrôler que les exigences sécurité techniques ou organisationnelles du CNRS sont satisfaites par les dispositions prises par le titulaire.

Les audits portent sur tout le périmètre du marché lié à une problématique de Sécurité, des audits partiels de Sécurité sont déclenchables à volonté par le CNRS.

Il est défini qu'il y aura un audit de Sécurité global au moment de la mise en place du marché.

Lors de l'exécution du marché, le CNRS peut décider la réalisation d'un tel audit (hors audits consécutifs à un incident de sécurité) au maximum une fois par période de douze (12) mois glissants.

Les audits peuvent être réalisés par le CNRS, ou délégué à un tiers. Ces contrôles s'effectueront par une visite des locaux du titulaire avec interviews individuelles des membres des équipes du titulaire, accès aux machines mises à la disposition du titulaire ou mises en œuvre par le titulaire.

Ces visites seront notifiées au titulaire cinq jours à l'avance.

En cas de survenance d'un incident de sécurité, le CNRS se réserve le droit d'effectuer ces contrôles sans préavis.

Le CNRS peut aussi réaliser ou faire réaliser à tout moment des tests de type intrusif. Le titulaire est informé deux jours à l'avance. Ces tests sont encadrés par une charte commune signée entre le titulaire, l'exécutant de l'audit et le CNRS. En cas de survenance d'un incident de sécurité, le CNRS se réserve le droit d'effectuer ces tests sans préavis.

Le CNRS se réserve le droit de requérir l'expertise du CERTA, de l'ANSSI ou d'une société tierce présentant des compétences en matière de sécurité.

Si le tiers mandaté est un Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le titulaire ne peut s'opposer à l'audit, à moins qu'il ne démontre que le tiers mandaté ne respecte pas le référentiel des exigences en vigueur.

Si le tiers mandaté n'est pas un PASSI qualifié par l'ANSSI, le titulaire peut s'opposer l'audit en indiquant au Pouvoir Adjudicateur les manquements au référentiel des exigences en vigueur qu'il reproche au tiers mandaté. Le Pouvoir Adjudicateur peut alors :

- Soit démontrer que ces reproches ne sont pas fondés
- Soit mandater un autre tiers pour procéder à l'audit.

Ces audits peuvent faire l'objet de plans de progrès sur le périmètre technique du marché et sur la gestion du marché.

6.3.5 Application des plans gouvernementaux

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

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

Le titulaire est tenu de mettre immédiatement en œuvre lesdites dispositions. Les conséquences financières de ces dispositions sont tirées soit par voie d'avenant, soit par les voies de droit.

6.3.6 Incident concernant les données à caractère personnel

En cas d'incident impliquant des données à caractère personnel, le titulaire doit informer le CNRS sans délai et lui fournir tous les éléments relatifs à cet incident dans un délai maximum de 48H.

7 DÉFINITION DES PRESTATIONS

Le présent marché est construit sur la base des prestations suivantes

Prestation	Nature	Renvoi
Prise en charge	Prestation Forfaitaire	Cf. § 7.1
Maîtrise d'œuvre déléguée	-	Cf. § 7.2
Réversibilité	Prestation Forfaitaire	Cf. § 7.3
Maintenance	Unitaire par classe de matériel	Cf. § 7.4
Supervision Des équipements et des vulnérabilités	Unitaire par type de matériel	Cf. § 7.5
Exploitation	Carnet de ticket mensuel	Cf. § 7.6
Catalogue de services	Prestation à prix unitaire par service	Cf. § 7.7
Expertises	Prestation à prix unitaire par H*J	Cf. § 7.8

7.1 PRISE EN CHARGE

7.1.1 Contenu de la prestation

Le titulaire et le CNRS définissent les modalités pratiques qui régissent le fonctionnement du marché.

Cela se traduira principalement par :

- La prise en charge de la maintenance (opération prioritaire)
- La mise en place des comités
- La définition du PAQ et PAS
- La mise en place des outils (gestion des incidents, gestion des demandes, monitoring, outillage technique d'administration et d'exploitation)
- La mise en place des procédures opérationnelles
- Une mise en place technique (équipements du titulaire, mise en place des liaisons, ouverture des accès).
- Durant cette période seront également définis plus précisément les éléments monitorés, graphés, les seuils d'alertes.
- Le titulaire peut solliciter la conduite d'un audit du réseau en place afin d'en valider l'architecture. La procédure est menée en coordination totale avec le CNRS, qui reste maître d'ouvrage de la procédure. Les résultats éventuels sont des livrables pour le CNRS.
- La récupération de tous les objets nécessaires au bon fonctionnement du marché dans le cadre de la réversibilité du titulaire sortant.

Cette prestation doit permettre une mise en place optimale du marché.

7.1.2 Modalités d'exécution

Cette phase de lancement doit se dérouler sur une période maximale d'un mois pour la partie maintenance (et gestion des incidents liés à celle-ci) et de deux mois pour la prise en main totale du marché.

7.1.3 Livrables et reporting

- PAQ
- PAS
- Maintenance des équipements renouvelée
- Ensemble des procédures opérationnelles
- Outillage mis en œuvre et opérationnel
- Infrastructures disponibles et opérationnelles sur le nouveau centre serveur.
- Les différentes matrices des droits et de contrôle d'accès

7.1.4 Contrat de service

NA

7.1.5 Pénalités

Lorsque la durée d'exécution du bon de commande est dépassée, le titulaire encourt, sans mise en demeure préalable, une pénalité de retard.

La durée d'exécution est stipulée dans le bon de commande.

Cette pénalité de retard est calculée par application de la formule suivante :

$$P = \left(\frac{V}{100} + 500 \right) \times R$$

Dans laquelle :

- P = montant des pénalités en Euros,
- V = valeur pénalisée, correspondant au montant H.T de la prestation commandée,
- R = nombre de jours calendaires de retard.

En cas de retard aboutissant à l'application de pénalités telles que P soit supérieur à 20 % du paiement relatif à la valeur pénalisée, il pourra être procédé à la résiliation du marché concerné aux torts du titulaire.

En tout état de cause, les pénalités sont appliquées dans la limite de ce seuil de 20%.

7.2 MAITRISE D'ŒUVRE DÉLÉGUÉE

7.2.1 Contenu de la prestation

La maîtrise d'œuvre déléguée est la prestation qui permet d'assurer un suivi contractuel et opérationnel du marché.

Elle est bâtie sur l'expression des besoins faite par le CNRS au §5 en termes :

- d'organisation
- de gouvernance
- de gestion du fond documentaire
- de récolte des indicateurs et de production de tableaux de bord.

7.2.2 Modalités d'exécution

La maîtrise d'œuvre déléguée qui contient en particulier les opérations de reporting, ne fait pas l'objet d'une Unité d'Œuvre dédiée. Elle est considérée comme incluse dans chacune des Unités d'Œuvre appliquée au périmètre des prestations.

Il en est de même pour les Prestations associées aux audits internes pour lesquels une participation du titulaire pourra être requis.

7.2.3 Livrables et reporting

- Tableaux de bord
- Compte-rendu des comités
- Documents inhérents au suivi du marché.

7.2.4 Contrat de service

Indicateur	Valeur attendue
Délais de fourniture des tableaux de bord et indicateurs	5 jours avant la tenue du comité
Délais de fourniture des CR des comités	5 jours après la tenue du comité

7.2.5 Pénalités

Cette pénalité de retard est calculée par application de la formule suivante :

$$P=200 \times R^2$$

Dans laquelle :

- P = montant des pénalités en Euros,
- R = nombre de jours calendaires de retard (plafonné à 5).

7.3 RÉVERSIBILITÉ

7.3.1 Contenu de la prestation

Cette prestation permet au titulaire de quitter le marché en laissant au CNRS et/ou au tiers mandaté les moyens de reprendre les différentes prestations de manière optimale.

7.3.2 Modalités d'exécution

Déclenchement à la demande du CNRS par notification d'un bon de commande exécutable sur une période de 2 mois.

7.3.3 Livrables et reporting

- L'ensemble des objets liés au marché dans leur dernière version
- Une sauvegarde de l'ensemble des configurations des équipements et les fichiers de configuration des outils de supervisions (Nagios, cacti, IP SLA ...)
- Tous les équipements du titulaire retirés des sites CNRS à la fin de la phase de réversibilité.
- Les PV de destructions et de restitutions des éléments appartenant au CNRS

7.3.4 Contrat de service

NA

7.3.5 Pénalités

Lorsque la durée d'exécution du bon de commande est dépassée, le titulaire encourt, sans mise en demeure préalable, une pénalité de retard.

Cette pénalité de retard est calculée par application de la formule suivante :

$$P = \left(\frac{V}{100} + 200 \right) \times R$$

Dans laquelle :

- P = montant des pénalités en Euros,
- V = valeur pénalisée, correspondant au montant H.T de la prestation de Réversibilité,
- R = nombre de jours calendaires de retard.

En tout état de cause, les pénalités sont appliquées dans la limite du seuil de 80% du cout de la prestation.

7.4 MAINTENANCE

7.4.1 Contenu de la prestation

Cette prestation permet la maintenance des équipements de l'inventaire.

7.4.2 Modalités d'exécution

Remplacement sur le site d'un équipement ou composant d'un équipement défectueux après diagnostic par le titulaire.

7.4.3 Livrables et reporting

- Remplacement de l'équipement ou du composant de l'équipement.
- Mise en place de la configuration est tests complets.
- Mise à jour des informations de gestion de parc.
- Reporting dans le cadre de la prestation de maîtrise d'œuvre délégué

7.4.4 Contrat de service

Pour une maintenance réalisée totalement par l'exploitant

Indicateur	Valeur attendue
Maintenance Standard	5J/7 (lundi-vendredi), heures de bureau (8 :00 – 18 :30), avec engagement de résultat à H+14 à partir du déclenchement de la maintenance (Décompté d'heure à heure)
Maintenance Médium	5J/7 (lundi-vendredi), heures de bureau (8 :00 – 18 :30), avec engagement de résultat à H+10 à partir du déclenchement de la maintenance
Maintenance Optimale	7J/7 (8 :00 – 18 :30), avec engagement de résultat à H+6 à partir du déclenchement de la maintenance
Maintenance Optimale +	7J/7 24h/24 avec engagement de résultat à H+6 à partir du déclenchement de la maintenance

Pour du support à la maintenance

Indicateur	Valeur attendue
Support à la Maintenance Standard	5J/7 (lundi-vendredi), heures de bureau (8 :00 – 18 :30), avec engagement de résultat à H+8 à partir de l'arrivée de l'équipement sur site (Décompté d'heure à heure)
Support à la Maintenance Médium	5J/7 (lundi-vendredi), heures de bureau (8 :00 – 18 :30), avec engagement de résultat à H+4 à partir de l'arrivée de l'équipement sur site
Support à la Maintenance Optimale	7J/7 (8 :00 – 18 :30), avec engagement de résultat à H+2 à partir du déclenchement de la maintenance ou de la réception de l'équipement sur site pour du « support à la maintenance »
Support à la Maintenance Optimale +	7J/7 24h/24 avec engagement de résultat à H+2 à partir de l'arrivée de l'équipement sur site

7.4.5 Pénalités

Lorsque la durée d'exécution de la prestation de Maintenance est dépassée, le titulaire encourt, sans mise en demeure préalable, une pénalité de retard.

Cette pénalité de retard est calculée par application de la méthode suivante :

- Maintenance ou support à la maintenance Standard :100 € par heure de retard au-delà de l'engagement
- Maintenance ou support à la maintenance Médium :400 € par heure de retard au-delà de l'engagement
- Maintenance ou support à la maintenance Optimale:1000 € par heure de retard au-delà de l'engagement
- Maintenance ou support à la maintenance Optimale +:2500 € par heure de retard au-delà de l'engagement

Les pénalités sont appliquées dans la limite de 12 heures de retard par action pénalisée.

7.5 SUPERVISION DES ÉQUIPEMENTS ET DES VULNÉRABILITÉS

7.5.1 Contenu de la prestation

Cette prestation a pour but :

- De surveiller les équipements en temps réel (disponibilité des équipements, disponibilité des liens, charge des équipements, charge des liens, qualité du réseau, performances du réseau, disponibilité des services rendus par l'équipement, anomalies de sécurité)
- De surveiller et analyser les avis et alertes de sécurité puis proposer un plan d'action.
- De détecter et résoudre les incidents.
- D'historiser les tickets

7.5.2 Modalités d'exécution

A la fin de la prestation de Prise en Charge, le titulaire est responsable de la supervision.

Les graphes peuvent être mis en place préalablement.

7.5.3 Livrables et reporting

Les équipements de supervision opérationnels.

Les graphes et l'outil de gestion des tickets accessibles.

7.5.4 Contrat de service

Indicateur	Traitement
Détection des incidents /ouverture ticket	24h/24 7j/7 avec une durée maximale annuelle d'indisponibilité de 8 heures de l'outillage de détection (superviseur et liaison(s) réseau du titulaire) sur douze mois. Ouverture du ticket ou indication de la prise en charge dans ticket existant dans les quinze minutes sur détection ou déclaration guichet unique.

Indicateur		Délais de résolution
Résolution des incidents	Mineur	16 heures ouvrées
	Majeur	4 heures en 24/7
	Critique	2 heures en 24/7

Indicateur	Traitement
Ouverture de ticket suite à CVE et analyse impact	Ouverture du ticket dans les 15mn 24h/24 7j/7. Analyse de la CVE dans les 1 heures 24h/24 7j/7 pour CVSS-B(V4) ≥ 9 Analyse de la CVE dans les 4 heures ouvrées (8h-18h30) pour $9 > \text{CVSS-B(V4)} \geq 7$ Analyse de la CVE dans les 10 heures ouvrées (8h-18h30) pour $\text{CVSS-B(V4)} < 7$

7.5.5 Pénalités

Lorsque la durée du traitement d'un incident est dépassée, le titulaire encourt, sans mise en demeure préalable, une pénalité de retard.

Cette pénalité de retard est calculée par application de la méthode suivante :

- Dépassement de la durée maximale annuelle d'indisponibilité de 8 heures:
Pénalité appliquée aux dates anniversaire du marché : 1% du cout annuel du marché par tranche d'une heure
Les pénalités sont appliquées dans la limite de 20% du cout annuel.
- Ouverture de ticket sur détection ou appel : 500 € par quart d'heure de retard à partir d'un quart d'heure en 24h/24 7j/7 sur un incident critique. 150 € sur un incident majeur, 50 € sur un incident mineur
- Résolution des incidents Mineurs : 200 € par heure de retard au-delà de 16 heures ouvrées
- Résolution des incidents Majeurs : 600 € par heure de retard au-delà de 4 heures en 24h/24 7j/7
- Résolution des incidents Critiques : 2000 € par heure de retard au-delà de 2 heures en 24h/24 7j/7

Ces pénalités sont appliquées dans la limite de 15 heures de retard par incident pénalisé

- Ouverture de ticket sur Alerte constructeur ou alerte des CERT définis dans PAS : 500 € par quart d'heure de retard à partir d'un quart d'heure en 24h/24 7j/7 sur CVSS-B \geq 9, 150 € sur 9>CVSS-B \geq 7, 50 € sur CVSS-B<7
- Mise a disposition du rapport d'analyse et plan d'action :
- CVSS-B<7 : 200 € par heure de retard au-delà de 10 heures ouvrées (8h-18h30)
- sur 9>CVSS-B \geq 7 : 600 € par heure de retard au-delà de 4 heures ouvrées (8h-18h30)
- sur CVSS-B \geq 9 : 2000 € par heure de retard au-delà de 1 heures en 24h/24 7j/7

Ces pénalités sont appliquées dans la limite de 15 heures de retard par incident pénalisé

7.6 EXPLOITATION

7.6.1 Contenu de la prestation

Cette prestation permet l'exploitation des équipements inclus dans le périmètre du titulaire :

- Gestion des configurations.
- Gestion des changements.
- Gestion des versions.

7.6.2 Modalités d'exécution

À la fin de la prestation de Prise en Charge, le titulaire est responsable de l'exploitation.

7.6.3 Livrables et reporting

L'état des versions du parc.

L'outillage de comparaison de configurations.

Les procédures de gestion de changements.

Les coordonnées des interlocuteurs.

7.6.4 Contrat de service

Indicateur	Traitement
Prise en compte d'une demande de changement.	Ouverture du ticket ou indication de la prise en charge dans un ticket existant dans les quinze minutes

Indicateur		Délais de traitement	
Gestion des demandes de changements		Normal	Urgent (25% max)
	Simple	4 heures ouvrées	2 heures ouvrées
	Médium	8 heures ouvrées	4 heures ouvrées
	Complexe	Défini lors de la demande (maximum 16h ouvrées)	

7.6.5 Pénalités

Lorsque la durée d'exécution d'une demande est dépassée, le titulaire encourt, sans mise en demeure préalable, une pénalité de retard.

Cette pénalité de retard est calculée par application de la méthode suivante :

- Ouverture de ticket : 50 € par quart d'heure de retard à partir d'un quart d'heure en heures ouvrées
- Les pénalités sont appliquées dans la limite de 4 heures de retard par incident pénalisé.

Réalisation des demandes :

- 100 € par heure de retard entre la 1^{ère} et 4^{ème} heure ouvrée de dépassement
- 200 € par heure de retard entre la 4^{ème} et 8^{ème} heure ouvrée de dépassement
- 500 € par heure de retard au-delà de la 8^{ème} heure de dépassement

Dans le cadre du traitement urgent, on applique un coefficient multiplicateur de 2.

Les pénalités sont appliquées dans la limite de 15 heures de retard par demande pénalisée.

Sauvegarde :

Sauvegarde d'un équipement non disponible ou impossibilité de mettre en place une sauvegarde sur un équipement.

- Dès lors qu'un incident apparaît dans le mois : 4000 € + 500 € par problème

Les pénalités sont appliquées dans la limite de 15 problèmes par mois pénalisé.

7.7 CATALOGUE DE SERVICES

En dehors des opérations récurrentes, sont définies ci-dessous un ensemble de tâches qui peuvent être commandées ponctuellement au titulaire

7.7.1 Intervention sur site SIREs

Nature	Descriptif
Mise en place / remplacement d'un ou plusieurs équipements sur un site SIREs	<p>Consiste à la mise en place d'un équipement sur un des sites de CNRS. L'intervenant devra placer l'équipement dans un rack d'une salle informatique. Câbler l'équipement tant au niveau électrique que réseau</p> <p>L'équipement devra être configuré avec la configuration fournie par l'équipe réseau de la DSI pour un nouveau matériel ou avec la configuration de l'équipement remplacé fourni par le système de gestion de configuration du titulaire.</p> <p>L'accès aux équipements par les équipes d'exploitation du titulaire devra être testé.</p>

7.7.2 Services relevant de l'exploitation des équipements

Des interventions le week-end ou en soirée peuvent être requises pour des opérations exceptionnelles sur le réseau. Ces interventions seront planifiées à minima une semaine à l'avance. Le titulaire fournit un ou des intervenants adaptés à la complexité des interventions dans ce délai.

Nature	Descriptif
Extension de la plage horaire d'exploitation	<p>Ces extensions doivent permettre d'étendre, pour des besoins ponctuels, les prestations d'administration et les engagements associés du titulaire au-delà des plages standards</p> <p>Elles seront déclinées :</p> <ul style="list-style-type: none"> Sur trois profils adaptés aux niveaux de complexité <ul style="list-style-type: none"> Profil Junior Profil Senior Profil Expert Sur 5 types d'extension de la plage <ul style="list-style-type: none"> Extension jour ouvré – 0 :00 – 24 :00 Extension samedi – 9 :00 – 18 :00 Extension samedi – 0 :00 – 24 :00 Extension dimanche – 9 :00 – 18 :00 Extension dimanche – 0 :00 – 24 :00
Audit d'une liaison	<p>Des mesures de qualité des liaisons pourront également être demandées au titulaire entre deux équipements qu'il administre. Cela pourra être fait grâce à la mise en place de sonde ou en utilisant les fonctionnalités incluses dans les équipements gérés. (La méthodologie aura été indiquée).</p> <p>Ces tests donneront lieu à un document de synthèse présentant entre autres :</p> <ul style="list-style-type: none"> Gigue Latence (source -> destination et destination -> source) Erreurs MTU Bande passante disponible. Stabilité du lien sur plusieurs jours.

7.7.3 Modalités d'exécution

A la demande lors des comités opérationnels ;

7.7.4 Livrables et reporting

Équipements/scripts en place et fonctionnels.

7.7.5 Contrat de service

NA

7.8 EXPERTISES

7.8.1 Contenu de la prestation

Dans les cas où cette prestation ne peut être confiée à un autre prestataire car ne pouvant être techniquement ou économiquement séparée du présent marché sans inconvénient majeur pour lui, le CNRS peut être amené à demander des prestations d'expertise sur une évolution d'architecture, audit d'une architecture existante ou autre.

Nature	Descriptif
Expertise/Etude	<ul style="list-style-type: none">• Profil Junior < 5 ans d'expérience en ingénierie réseau• Profil Senior > 10 ans d'expérience en ingénierie réseau• Profil Expert > 10 ans d'expérience dans la technologie source de la prestation Par journée / 3 jours / semaine

7.8.2 Modalités d'exécution

- Précisé à la commande de la prestation

7.8.3 Livrables et reporting

- Rapport de présentation du résultat de la prestation

7.8.4 Contrat de service

NA