



Plan d'Assurance Sécurité

Conforme ISO 27002-2013

Présentation du PAS

Version 1.0 – Jan 2025

Historique des versions

Version - Date	Emetteur	Statut/Suivi des modifications
1.0 - Jan 2025	DCISN Fabien MALBRANQUE	Version initiale.

Objectif du document	Plan d'assurance sécurité à faire compléter et signer par les prestataires.
Mots clefs	Conformité SSI des prestations.
Résumé	Le Plan d'Assurance de Sécurité de l'information (nommé ci-après PAS) rassemble tous les contrôles de sécurité et des services de sécurité acceptés et contractés afin de garantir les conditions de sécurité exigées dans les prestations commanditées par la CNAF / CAF.

Sommaire

1. INTRODUCTION	5
2. PERIMETRE D'APPLICATION DE LA SECURITE	5
3. PRESENTATION DU DOCUMENT	6
4. STRUCTURE DU DOCUMENT	6
5. LES DOCUMENTS DE REFERENCE	7
6. DESCRIPTION DE LA PRESTATION (A COMPLETER)	7
7. APPLICATION DU PAS	8
7.1 PORTEE DU PAS	8
7.2 PROCEDURE EN CAS DE NON-APPLICATION ET DEMANDE DE DEROGATION	8
7.3 PROCEDURE DE CONTROLE DU RESPECT DU PAS	8
7.4 PROCEDURE EN CAS DE NON-RESPECT DU PAS	8
8. MESURES DE SECURITE	9
8.1 POLITIQUE DE SECURITE DE L'INFORMATION	9
8.1.1 <i>Politique de sécurité de l'information</i>	9
8.2 ORGANISATION DE LA SECURITE DE L'INFORMATION SI	10
8.2.1 <i>Organisation Interne</i>	10
8.2.2 <i>appareils mobiles et télétravail</i>	12
8.3 SECURITE LIEE AUX RESSOURCES HUMAINES	13
8.3.1 <i>Sécurité liée aux ressources humaines</i>	14
8.3.2 <i>Formation aux procédures de sécurité du personnel</i>	15
8.3.3 <i>Rupture, terme ou modification du contrat de travail</i>	16
8.3.4 <i>Localisation des collaborateurs du prestataire</i>	17
8.3.5 <i>Gestion des arrivées et des départs</i>	17
8.3.6 <i>Recours à la sous-traitance</i>	19
8.3.7 <i>Recours au personnel extérieur</i>	20
8.4 GESTION DES ACTIFS	20
8.4.1 <i>Responsabilités relatives aux actifs</i>	20
8.4.2 <i>Classification de l'information</i>	21
8.5 CONTROLE D'ACCES	22
8.5.1 <i>Exigences métier en matière de contrôle d'accès</i>	22
8.5.2 <i>Gestion de l'accès utilisateur</i>	24
8.5.3 <i>Responsabilités des utilisateurs</i>	26

8.5.4	<i>contrôle de l'accès au système et aux applications</i>	27
8.6	CRYPTOGRAPHIE	29
8.7	SECURITE PHYSIQUE ET ENVIRONNEMENTALE	30
8.7.1	<i>Zones sécurisées</i>	30
8.7.2	<i>Matériels</i>	30
8.8	SECURITE LIEE A L'EXPLOITATION	32
8.8.1	<i>Procédures et responsabilités liées à l'exploitation</i>	32
8.8.2	<i>Protection contre les logiciels et codes malveillant et mobile</i>	34
8.8.3	<i>Sauvegarde</i>	36
8.8.4	<i>Journalisation et surveillance</i>	36
8.8.5	<i>Maîtrise des logiciels en exploitation</i>	38
8.8.6	<i>Gestion des vulnérabilités techniques</i>	39
8.8.7	<i>Considérations sur l'audit des systèmes d'information</i>	40
8.9	SECURITE DES COMMUNICATIONS	41
8.9.1	<i>Management de la sécurité des réseaux</i>	41
8.9.2	<i>Transfert de l'information</i>	43
8.10	ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION	45
8.10.1	<i>Exigences de sécurité applicables aux systèmes d'information</i>	45
8.10.2	<i>Sécurité des processus de développement et d'assistance technique</i>	46
8.10.3	<i>Données de test</i>	48
8.11	GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION	48
8.11.1	<i>Gestion des incidents liés à la sécurité de l'information et améliorations</i>	48
8.12	ASPECTS DE LA SECURITE DE L'INFORMATION DANS LA GESTION DE LA CONTINUITE DE L'ACTIVITE	51
8.12.1	<i>Continuité de la sécurité de l'information</i>	51
8.12.2	<i>Redondance</i>	53
8.13	CONFORMITE	54
8.13.1	<i>Conformité aux obligations légales et réglementaires</i>	54
8.13.2	<i>Revue de la sécurité de l'information</i>	56
9.	MESURES COMPLEMENTAIRES A L'ISO 27002	58
9.1	UTILISATION DE L'INTELLIGENCE ARTIFICIELLE (IA)	58
9.1.1	<i>Interdiction de l'usage de l'IA</i>	58
9.1.2	<i>Demande d'autorisation de l'usage de l'IA</i>	59

1. INTRODUCTION

Dans ce document, la société chargée des prestations de service pour le compte de la CNAF / CAF sera identifiée comme étant le « Prestataire ». Le Plan d'Assurance de Sécurité de l'information (nommé ci-après PAS) rassemble tous les contrôles de sécurité et les services de sécurité acceptés et contractés afin de garantir les conditions de sécurité exigées dans les prestations commanditées par la CNAF / CAF. Il est sous la responsabilité du Directeur de la DCISN (Direction du Contrôle Interne et de la Sécurité du Numérique) de la DSI de la CNAF / MSSI (Manager de la Sécurité du Système d'Information) de la CAF.

Sur la base de ce PAS, le « Prestataire » doit définir, mettre en œuvre et opérer les services de sécurité, les procédures, les processus, l'organisation, les infrastructures et les outils. Les responsabilités seront définies tant au niveau opérationnel que pour toutes les phases des projets qui lui sont confiés (la conception, la transformation et l'exploitation) et cela pour tous les contrôles de sécurité, les exigences et les paramètres spécifiques.

Le PAS sera utilisé par les diverses équipes opérationnelles pour gérer la prestation de services de sécurité au travers des technologies déployées, des organisations et des processus.

Le PAS est inclus dans le contrat comme un programme. Dans ce cadre, le PAS est un document contractuel engageant le « Prestataire » et sa Direction Technique quant à la fourniture des services de sécurité décrits ci-après.

Le PAS sera revu et complété durant la phase de mise en œuvre de la prestation et une première version finalisée sera livrée avant le démarrage du projet en production.

Les références utilisées par la CNAF / CAF suivent les chapitres du référentiel ISO/IEC 27002:2013.

2. PERIMETRE D'APPLICATION DE LA SECURITE

Ce document s'applique aux prestations SI réalisées pour le compte de la CNAF / CAF. Le « Prestataire » s'engage à ce que la prestation de réalisation ainsi que les livrables résultants respectent les exigences exposées dans le présent document. Le périmètre d'application de la sécurité pour le contrat est le suivant :

- La sécurité appliquée à la réalisation des prestations (organisation, gouvernance, pilotage) ;
- Le pilotage de la sécurité dans la réalisation des prestations ;

Le cas échéant :

- La sécurité des environnements et des équipements du « Prestataire » mis en place pour la CNAF / CAF ;
- La sécurité des environnements et des équipements que la CNAF / CAF met à disposition du « Prestataire » ;
- La sécurité du développement des briques applicatives des SI de la CNAF / CAF.

3. PRESENTATION DU DOCUMENT

Ce document est issu de l'appropriation du standard international ISO/IEC 27002:2013, Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la gestion de la sécurité de l'information, comme cadre pour fournir la sécurité de l'information.

Pour les 14 chapitres de la norme ISO/IEC 27002:2013, décrits ci-après, ce document détaille les exigences de sécurité du RSSI de la CNAF / MSSI de la CAF.

- Le document décrit les rôles et responsabilités de chacune des parties (la CNAF / CAF et Prestataire).
- Pour chaque clause, le Prestataire confirme sa capacité de satisfaire aux exigences comme indiqué dans le chapitre III du document et indique si ces services sont compris dans la prestation (services Standard) ou peuvent être activés en plus en cas de besoin (Option).
- Le Prestataire s'engage à répondre aux exigences de sécurité de la CNAF / CAF et accepte totalement le partage des responsabilités ainsi que les besoins exprimés.
- Le Prestataire accepte d'être audité par la CNAF / CAF ou par une entreprise mandatée et de fournir toutes les informations, preuves, relatives et applicables à ce PAS (les procédures, les processus, l'organisation ou de la documentation technique) afin de vérifier les engagements et les services du Prestataire (conformément à la clause d'audit générale définie dans le contrat maître).

4. STRUCTURE DU DOCUMENT

La partie 4 décrit les exigences de sécurité de la CNAF / CAF. Elles sont partagées indépendamment de la capacité du Prestataire à mettre en œuvre ou non les mesures de sécurité.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
<i>Exigence applicable par le prestataire</i>			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.</i>				

- « **Chapitre ISO** » donne la référence du chapitre ISO 27002. Lorsque des adaptations sont requises pour une mesure, une étoile (*) est ajoutée ;
- « **Service** » décrit si la mesure doit être mise en œuvre (obligatoire) ou, selon le niveau de criticité, peut être évitée (en option) ;
 - Obligatoires : les services obligatoires sont les services de sécurité couvrant les risques qui ne peuvent pas être acceptés par la CNAF / CAF et qui doivent être réduits par la mise en œuvre des mesures quel que soit le projet ou l'infrastructure ;
 - En option : à la suite d'une évaluation des risques et l'analyse des résultats, certains risques peuvent être acceptés par la CNAF / CAF pour certains projets spécifiques, les infrastructures, etc., et donc ne sont pas réduits par des mesures dédiées ;
- « **Mesure** » est une description du contrôle de l'ISO 27002 ou d'exigences normatives au sein des guides et référentiels notamment de l'ANSSI. Elle décrit fonctionnellement le contrôle concerné sans pour autant préciser la manière de l'implémenter ;
- « **Prestataire** » indique ce qui est de la responsabilité du Prestataire sans pour autant être

exhaustif ;

- « **CNAF / CAF** » indique ce qui est de la responsabilité de l'organisme de la branche ;
- « **Exigence applicable par le prestataire** » : Le prestataire indique s'il est en mesure d'appliquer strictement l'exigence. Dans le cas contraire, il indique ce qu'il met en œuvre et comment il le met. Dans le cas où cette exigence ne concerne pas la prestation, il coche « NON »

Chapitre ISO	Adaptation	Exigences de la CNAF / CAF

- « **Chapitre ISO** » est la référence au standard ISO 27002 ;
- « **Adaptation** » est une mesure identifiée comme spécifique ou non décrite dans le standard ISO ;
- « **Exigences de la CNAF / CAF** » décrivent les spécificités demandées.

5. LES DOCUMENTS DE REFERENCE

Nom du document	Référence
Politique de Sécurité des Systèmes d'Information du Ministère chargé des affaires sociales	PSSI_MCAS
Politique de Sécurité des Systèmes d'Information de la CNAF	PSSI-CNAF
Référentiel général de sécurité (RGS)	RGS
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016	RGPD
Loi n° 78-17 du 6 janvier 1978 modifiée par le décret n°2019-536 du 29 mai 2019 et relative à l'informatique, aux fichiers et aux libertés	Loi Informatique et Libertés
Norme ISO 27001	ISO-27001:2013
Référentiel ISO 27002	ISO-27002:2013

6. DESCRIPTION DE LA PRESTATION (à compléter)

Le service rendu par le prestataire

- *Fournir un récapitulatif de la ou des prestations prévues initialement dans le mémoire technique*
- *Description des systèmes d'informations utilisés pour la ou les prestations*

7. APPLICATION DU PAS

Les exigences de sécurité identifiées et prises en compte dans le cadre du contrat, du marché sont issues des documents de référence listés au chapitre 5.

7.1 PORTEE DU PAS

Les acteurs du projet sont tenus d'appliquer les dispositions décrites dans le présent Plan d'Assurance Sécurité.

7.2 PROCEDURE EN CAS DE NON-APPLICATION ET DEMANDE DE DEROGATION

Le RSSI de la CNAF / MSSI de la CAF et le RSSI du prestataire sont les seules personnes habilitées à émettre des demandes de dérogations. Chaque dérogation au PAS fait l'objet d'une demande sous la forme d'un document qui expose :

- La dérogation souhaitée aux règles de sécurité ;
- Les risques encourus ;
- Les moyens qu'il est souhaitable d'engager afin de réduire ces risques ;
- La durée de dérogation souhaitée.

La demande de dérogation est instruite par le RSSI de la CNAF / MSSI de la CAF.

7.3 PROCEDURE DE CONTROLE DU RESPECT DU PAS

Le Plan d'Assurance Sécurité fait l'objet d'un suivi régulier exercé par la CNAF / CAF et le prestataire. Les contrôles sont réalisés à intervalles programmés (i.e. lors de comité sécurité) ou en cas de changement majeur.

7.4 PROCEDURE EN CAS DE NON-RESPECT DU PAS

Le « Prestataire » s'engage à respecter et à faire respecter par le personnel travaillant sur la ou les prestations, les règlements et les règles de sécurité exprimées ou rappelées dans le Plan Assurance Sécurité jusqu'à la cessation complète du contrat.

Toute non-conformité relevée par l'une ou l'autre des parties doit :

- Être accompagnée d'un compte-rendu indiquant la non-conformité au regard du référentiel d'exigences. Cette action est à la charge de l'acteur ayant découvert la non-conformité de la CNAF / CAF ou du « Prestataire » ;
- Être adressée à l'autre partie ;
- La non-conformité doit être analysée afin d'évaluer les risques et impacts potentiels au regard des intérêts de la CNAF / CAF et des personnes. Cette action est à la charge de l'acteur à l'origine de la non-conformité. Suivant les résultats de l'analyse, la CNAF / CAF ou le « Prestataire » engage une action corrective qui peut être :
 - La mise en conformité des défauts constatés ;
 - La correction apportée au PAS ;
 - L'émission d'une demande de dérogation si la non-application est justifiée.

- Faire l'objet d'une information au comité de pilotage. Cette action est à la charge de l'acteur à l'origine de la non-conformité.
- L'action corrective est actée dans le « Compte rendu du Comité de Sécurité ».

8. MESURES DE SECURITE

8.1 POLITIQUE DE SECURITE DE L'INFORMATION

8.1.1 POLITIQUE DE SECURITE DE L'INFORMATION

Objectif : Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier, aux lois et aux réglementations en vigueur.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
5.1.1*	Obligatoire	Politiques de sécurité de l'information. Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.	<ul style="list-style-type: none"> ▪ Présente sa politique de sécurité de l'information (PSI) aux représentants du RSSI de la CNAF / MSSI de la CAF. ▪ Selon la nature de la prestation, produit éventuellement des spécifications techniques. ▪ Implémente le "PAS" (et éventuellement les spécifications techniques). 	<ul style="list-style-type: none"> ▪ Approuve et valide le PAS et éventuellement les spécifications techniques
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.</i>				
5.1.2	Obligatoire	Revue des politiques de sécurité de l'information. Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs.	<ul style="list-style-type: none"> ▪ Répond aux changements ou dérogations accordées par le RSSI de la CNAF / MSSI de la CAF. ▪ Est respectueux des lois et des réglementations (limitées à la sécurité de l'information gérée par le Prestataire). ▪ Fournit un plan d'amélioration en cas de manquement au PAS. ▪ Analyse les contraintes et propose de nouveaux services si nécessaire. 	<ul style="list-style-type: none"> ▪ Revoit régulièrement les politiques de sécurité ▪ Informe le Prestataire en cas d'évolution des exigences ou de besoin de dérogation. ▪ Approuve et valide les changements ou les dérogations du "PAS". ▪ Valide le plan d'amélioration.

Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</p> <p>Justification lorsque le prestataire juge la mesure non applicable.</p>				
Chapitre ISO	Adaptation	Exigences de la CNAF / CAF		
5.1.1	Politiques de sécurité de l'information.	Le prestataire fournira à la CNAF / CAF, le cas échéant, les certifications d'entreprise (par exemple du type ISO 27001) en précisant le périmètre concerné.		
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</p> <p>Justification lorsque le prestataire juge la mesure non applicable.</p>				

8.2 ORGANISATION DE LA SECURITE DE L'INFORMATION SI

8.2.1 ORGANISATION INTERNE

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
6.1.1	Obligatoire	Fonctions et responsabilités liées à la sécurité de l'information. Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.	<ul style="list-style-type: none"> Le Prestataire identifie un RSSI pour la prestation. Met en place un comité de sécurité 	<ul style="list-style-type: none"> Identifie un correspondant sécurité de l'information pour la prestation Définit la fréquence du comité de sécurité
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</p> <p>Justification lorsque le prestataire juge la mesure non applicable.</p>				
6.1.2	Obligatoire	Séparation des tâches. Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.	<ul style="list-style-type: none"> Implémente des contrôles pour s'assurer du niveau de ségrégation Fournit les éléments d'audit 	<ul style="list-style-type: none"> Définit les fonctions et les domaines de responsabilité Fournit des exigences spécifiques

Exigence applicable par le prestataire					OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>						
6.1.3*	Obligatoire	Relations avec les autorités. Des relations appropriées avec les autorités compétentes doivent être entretenues.	<ul style="list-style-type: none"> Fournit les informations appropriées afin de permettre à la CNAF / CAF de répondre aux requêtes des autorités Transmet à la CNAF / CAF, toutes requêtes des autorités. 	<ul style="list-style-type: none"> Transmet au Prestataire toutes requêtes des autorités 		
Exigence applicable par le prestataire					OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>						
6.1.4	Obligatoire	Relations avec des groupes de travail spécialisés. Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues.	<ul style="list-style-type: none"> Maintient la liste des relations des organisations, des fournisseurs, des professionnels, etc. spécialisés dans la sécurité de l'information, pour garder un niveau d'expertise. 	<ul style="list-style-type: none"> Pas d'action 		
Exigence applicable par le prestataire					OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>						
6.1.5	Obligatoire	La sécurité de l'information dans la gestion de projet. La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type (applicatif, infrastructure).	<ul style="list-style-type: none"> Implémente les mesures de sécurité. 	<ul style="list-style-type: none"> Suit l'implémentation 		
Exigence applicable par le prestataire					OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>						

Chapitre ISO	Adaptation	Exigences de la CNAF / CAF
6.1.3	Relations avec les autorités.	Le Prestataire doit informer la CNAF / CAF, des requêtes des autorités, concernant des informations ou des équipements appartenant à la CNAF / CAF ou ayant un impact sur l'activité de la CNAF / CAF (saisie de l'équipement ou des données partagées).
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.2.2 APPAREILS MOBILES ET TELETRAVAIL

Objectif : Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
6.2.1 – 6.2.2	Obligatoire	Appareils mobiles et télétravail. Le prestataire adopte une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles et de la mise en place du télétravail.	<ul style="list-style-type: none">▪ Met en place une politique de sécurisation des matériels mobiles▪ Définit les conditions et les restrictions liées au télétravail	<ul style="list-style-type: none">▪ Pas d'action
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				

Chapitre ISO	Adaptation	Exigences de la CNAF / CAF
6.2.*	Appareils mobiles et télétravail	<p>Le prestataire est responsable de gérer ses propres contrôles et afin de faciliter les interventions et les respects des SLA, le personnel du prestataire pourra se connecter à distance au SI aux seules conditions suivantes, et sans préjudice des autres principes fondamentaux énumérés dans ce document.</p> <ul style="list-style-type: none"> Mise en œuvre d'une communication chiffrée et authentifiée à partir d'un poste de travail avec gestion centralisée configuré comme suit : <ul style="list-style-type: none"> Boot uniquement sur le DD interne de la machine, Activation du « Secure Boot », Bios verrouillé avec mot de passe, S'il contient des données relatives au SI de la CNAF / CAF (adresses IP, mots de passe etc.), chiffrement des données du DD de la machine de préférence avec un produit

		<p>certifié critères communs EL2+ minimum,</p> <ul style="list-style-type: none"> ○ Authentification à 2 facteurs de l'utilisateur (de préférence basée sur un certificat) pour ouvrir une session sur la machine distante, ○ Présence d'une protection antimalware à jour, ○ Présence d'un pare-feu à jour, ○ Présence d'un système d'exploitation maintenu par l'éditeur, ○ Durcissement du système d'exploitation selon les recommandations de l'ANSSI, Mise à jour des patches de sécurité de tous les logiciels. <ul style="list-style-type: none"> ● En nomadisme, un filtre de confidentialité doit être utilisé. <p>Il est de la responsabilité du prestataire de fournir des terminaux mobiles sécurisés à ses équipes s'ils sont utilisés pour accéder à des ressources du RSSI de la CNAF / MSSI de la CAF.</p> <p>Ces terminaux doivent à minima inclure :</p> <ul style="list-style-type: none"> ● Un système d'exploitation à jour (et patches de sécurité) et non jailbreaké/root, ● L'utilisation d'un mot de passe ou d'une méthode de verrouillage robuste, ● La protection du terminal mobile par du chiffrement. <p>Le Prestataire doit également sensibiliser son personnel aux bonnes pratiques de protection de leur poste de travail.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.3 SECURITE LIEE AUX RESSOURCES HUMAINES

Objectif de ce chapitre : Les collaborateurs de la CNAF / CAF et du Prestataire comprennent les enjeux et leurs responsabilités. Ils sont compétents pour leurs fonctions et contribuent à réduire le risque de vol, de fraude ou d'usage malveillant des moyens mis à disposition.

Ils sont conscients des menaces et conséquences portant sur la sécurité de l'information, de leurs responsabilités. Ils sont capables de soutenir la politique de sécurité de l'entreprise dans le cadre de leur travail normal, de réduire les risques d'erreur humaine.

Le prestataire gère correctement le changement d'emploi ou le départ de son personnel.

Le personnel du prestataire reste en toutes circonstances sous son autorité hiérarchique et disciplinaire. Le prestataire assure donc, en sa qualité d'employeur, la gestion administrative, comptable et sociale de ses salariés intervenant dans l'exécution de la ou des prestations prévues au contrat.

8.3.1 SECURITE LIEE AUX RESSOURCES HUMAINES

Objectif : S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
7.1.1	Obligatoire	Sélection des candidats. Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés	<ul style="list-style-type: none"> Est responsable de la sélection de ses employés, indépendamment des moyens de vérification Garde une trace des preuves associées Fournit les informations demandées nécessaire pour les enquêtes à la suite d'un incident de sécurité 	<ul style="list-style-type: none"> Pour les besoins d'une enquête sur un incident de sécurité, fournit les renseignements pertinents
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i>				
7.1.2*	Obligatoire	Termes et conditions d'embauche. Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.	<ul style="list-style-type: none"> Inclut des obligations contractuelles de sécurité de l'information dans les contrats de tous les employés ou sous-traitants du Prestataire Fournit une liste des obligations de sécurité incluses dans les contrats 	<ul style="list-style-type: none"> Pas d'action
Exigence appliquée par le prestataire				
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Adaptation	Exigences de la CNAF / CAF
--------------	------------	----------------------------

7.1.2	Termes et conditions d'embauche	<p>Accord contractuel relatif à la sécurité de l'information (non limité à) :</p> <ul style="list-style-type: none"> ▪ Confidentialité ; ▪ Accord de non-divulgaration ; ▪ Respect de la propriété intellectuelle. <p>Les collaborateurs du prestataire s'engagent en complément de leur contrat de travail, à respecter les chartes informatiques (utilisateurs et/ou administrateurs) de la CNAF / CAF.</p>
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>		
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.3.2 FORMATION AUX PROCEDURES DE SECURITE DU PERSONNEL

Objectif : S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
7.2.2*	Obligatoire	Sensibilisation, apprentissage et formation à la sécurité de l'information. L'ensemble des salariés de l'organisation et des contractants suivent un apprentissage et des formations de sensibilisation adaptés et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.	<ul style="list-style-type: none"> ▪ Est responsable du programme des formations de sensibilisation à la sécurité de ses employés et de ses contractants ▪ Etablit et planifie un programme de sensibilisation adapté selon la fonction des employés et contractants 	<ul style="list-style-type: none"> ▪ Pas d'action
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée</i></p>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
7.2.2	En cours d'emploi. Les employés et les contractants reconnaissent et assument leurs responsabilités en matière de sécurité de l'information.	<ul style="list-style-type: none"> ▪ Il est de la responsabilité du Prestataire de gérer ces contrôles ▪ Des mesures doivent être mises en place pour sensibiliser le personnel concerné, des conséquences possibles : <ul style="list-style-type: none"> ○ Sur la gestion des données à caractère personnel (par exemple, les conséquences juridiques, perte de l'entreprise et de la marque ou de dommages à la réputation), ○ Sur le personnel (par exemple, les conséquences disciplinaires)

		<ul style="list-style-type: none"> ○ Sur le principe de protection d'information, du non-respect des règles et procédures de confidentialité ou de sécurité, notamment celles qui concernent le traitement des données à caractère personnel.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		
7.2.2	Sensibilisation et la formation Sécurité des collaborateurs du prestataire	<p>Le prestataire doit être en mesure de mettre en œuvre des campagnes de sensibilisation à minima sur les thèmes relatifs à la cybersécurité au moyen de session de E-Learning ou de formation :</p> <ul style="list-style-type: none"> • Les Risques et les menaces ; • Les Conséquences d'une corruption des données ; • Internet, courriel et média social ; • Data Privacy ; • OWASP et vulnérabilités applicatives.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		
7.2.2	Suivi des sensibilisations et des formations	<p>Le prestataire doit mettre en place un workflow pour le suivi des formations afin d'en assurer la traçabilité. Cela permet aussi de réactualiser annuellement les pratiques Sécurité appliquées sur la prestation.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.3.3 RUPTURE, TERME OU MODIFICATION DU CONTRAT DE TRAVAIL

Objectif : Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
7.3.1*	Obligatoire	Achèvement ou modification des responsabilités associées au contrat de travail. Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en informer le salarié ou le	<ul style="list-style-type: none"> ▪ Met à jour la liste du personnel intervenant sur la prestation avec leur fonction sur le SI de la CNAF / CAF ou mis à disposition pour la CNAF / CAF avec leur localisation ▪ Fournit la liste du personnel intervenant après chaque 	<ul style="list-style-type: none"> ▪ Pas d'action

	contractant et de veiller à leur application.	modification	
Exigence applicable par le prestataire		OUI <input type="checkbox"/>	NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i>			

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail.	<ul style="list-style-type: none"> Responsabilité du Prestataire de gérer ces contrôles Réalisé des revus inverses des habilitations au moins une fois par an
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.3.4 LOCALISATION DES COLLABORATEURS DU PRESTATAIRE

	Paramètres	Exigences de la CNAF / CAF
	Territorialité	<p>Les collaborateurs du prestataire sont localisés :</p> <ul style="list-style-type: none"> Soit dans les locaux de la CNAF / CAF. A ce titre les collaborateurs du prestataire doivent respecter les règles de sécurité générale applicables dans les locaux de la CNAF / CAF au démarrage des prestations ; Soit dans les locaux du prestataire ; Soit à domicile dans le cadre du télétravail s'il est autorisé par la CNAF / CAF pour la réalisation des prestations du contrat à la condition que le lieu de réalisation soit dans l'union européenne.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.3.5 GESTION DES ARRIVEES ET DES DEPARTS

	Paramètres	Exigences de la CNAF / CAF
	Mesures prises lors des prestations	<p>Avant tout démarrage des prestations, le prestataire doit :</p> <ul style="list-style-type: none"> Fournir à la CNAF / CAF la liste des intervenants et des éventuels sous-traitants, ainsi que leur localisation,

		positionnés sur la prestation. Au cours des prestations, le prestataire doit : <ul style="list-style-type: none"> Fournir à la CNAF / CAF la liste à jour du personnel intervenant après chaque modification.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre pour y répondre		
	Paramètres	Exigences de la CNAF / CAF
	Mesures prises lors d'une fin de prestations	A la fin de toutes prestations, le prestataire doit systématiquement : <ul style="list-style-type: none"> S'engager à garantir, lors du transfert vers la CNAF / CAF, la sécurité et l'exhaustivité des données qui lui ont été confiées ; S'engager à restituer les données et les outils permettant d'y accéder, de les exploiter, a minima dans un format standard (par exemple .csv, .xml, .mp3, etc.) ; Assurer la destruction de tous les fichiers manuels ou informatisés stockant les informations de la CNAF / CAF, après l'accord de la CNAF / CAF ; Utiliser des outils d'effacement des données conformes à l'état de l'art (Standard Dod avec une surcharge 3 passes minimum) ; Fournir un rapport de destruction à la CNAF / CAF.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre pour y répondre		
	Mesures prises en début de mission	Avant tout démarrage d'une mission, le prestataire doit : <ul style="list-style-type: none"> Fournir à la CNAF / CAF la liste des intervenants à jour et des éventuels sous-traitants, ainsi que leur localisation, positionnés sur la mission ; Vérifier que son personnel est conscient des risques de sécurité et de leur responsabilité au travers d'un processus d'intégration sur la prestation.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description de la mesure en œuvre pour y répondre		
	Mesures prises en cours de mission	Le prestataire doit mettre en œuvre des mesures liées à la gestion du personnel prise au cours de la prestation telles que : <ul style="list-style-type: none"> Une communication à chaque évolution majeure des procédures et documents relatifs à la sécurité ; Tenir des revues périodiques permettant de contrôler le respect des règles de sécurité ; Contrôler en continu le respect des dispositions de sécurité par chaque collaborateur.

Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
	Mesures prises en fin de mission	<p>Les dispositions suivantes doivent être prises systématiquement lors du départ d'un collaborateur du prestataire :</p> <ul style="list-style-type: none"> • Restitution de l'ensemble des équipements fournis par la CNAF / CAF ; • Restitution du badge personnel à la CNAF / CAF ; • Destruction sécurisée de toutes les données de la CNAF / CAF présentes sur des supports amovibles et sur les matériels informatiques du prestataire mis à disposition de l'intervenant. Le prestataire doit fournir un procès-verbal de destruction en fin de mission.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.3.6 RECOURS A LA SOUS-TRAITANCE

Paramètres	Exigences de la CNAF / CAF
Sous-traitance	<p>En cas de recours à la sous-traitance dans le cadre de la prestation, la PSSI des entreprises relatives aux sous-traitants s'applique. Celle-ci doit identifier les contrôles de sécurité à réaliser et ceux à mettre en place :</p> <ul style="list-style-type: none"> • Le prestataire reportera l'ensemble des exigences et des contraintes de service à ses sous-traitants ; • Le prestataire avisera les sous-traitants des règles et des procédures spécifiques à respecter dans le cadre de leurs activités ; • La liste de l'ensemble des sous-traitants doit être construite et tenue à jour par le prestataire ; • La liste des sous-traitants doit être transmise à la CNAF / CAF à chaque mise à jour ; • Une clause de sécurité doit apparaître dans les contrats entre le prestataire et leurs sous-traitants. Celle-ci doit reprendre toutes exigences de sécurité relatives à la prestation.
<p>Exigence applicable par le prestataire</p> <p>OUI <input type="checkbox"/> NON <input type="checkbox"/></p>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	

8.3.7 RECOURS AU PERSONNEL EXTERIEUR

	Paramètres	Exigences de la CNAF / CAF
	Personnel extérieur	<p>Les intervenants des sociétés extérieures au titulaire assurant une prestation, une maintenance ou un support technique de solution doivent être accompagnés par une personne habilitée du titulaire à intervenir sur le système pendant toute la durée de leur intervention.</p> <p>Le titulaire doit mettre en œuvre les mesures techniques et organisationnelles pour empêcher toute extraction ou récupération d'informations électroniques ou papiers par la présence d'une clause de confidentialité dans le contrat du personnel intervenant dans les locaux dédiés à l'exécution des prestations.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.4 GESTION DES ACTIFS

Objectif de ce chapitre : La gestion des actifs permet d'atteindre et maintenir une protection adéquate des actifs de la CNAF / CAF.

8.4.1 RESPONSABILITES RELATIVES AUX ACTIFS

Les propriétaires doivent être identifiés pour tous les actifs et leurs responsabilités doivent leur être signifiées pour apporter le niveau de protection adéquat aux actifs.

La gestion des actifs permet à ces derniers de recevoir un niveau approprié de protection selon sa classification afin d'identifier les besoins de sécurité et le degré de protection attendu.

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
8.1.*	Responsabilité des actifs	La mise en œuvre et le respect des mesures pertinentes, selon la norme ISO, pour la gestion des actifs, concernés par le service, sont de la responsabilité du Prestataire.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.4.2 CLASSIFICATION DE L'INFORMATION

Objectif : L'information bénéficie d'un niveau de protection approprié conforme à son importance pour la CNAF / CAF.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
8.2.1	Obligatoire	Classification des informations : Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.	<ul style="list-style-type: none"> Identifie les données sensibles en fonction des spécifications de la CNAF / CAF 	<ul style="list-style-type: none"> Définit et maintient les règles de classification et de déclassification de l'information. Fournit l'inventaire des données sensibles concernées par le périmètre de la prestation.
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
8.2.2	Obligatoire	Marquage des informations : Un ensemble approprié de procédures de marquage de l'information doit être élaboré conformément au plan de classification adopté par l'organisation.	<ul style="list-style-type: none"> Met en œuvre les politiques et les mesures de protection et de gestion des données sensibles 	<ul style="list-style-type: none"> Pas d'action
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
8.2.3	Obligatoire	Manipulations des actifs : Des procédures de traitement de des actifs doivent être élaborées et mises en œuvre conformément au plan de classification de l'information adopté par l'organisation.	<ul style="list-style-type: none"> Met en œuvre les politiques et les mesures de protection et de gestion des actifs 	<ul style="list-style-type: none"> Pas d'action
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

	Paramètres	Exigences de la CNAF / CAF
	Gestion des matériels fournis aux collaborateurs du prestataire	<p>La CNAF / CAF fournit éventuellement des postes de travail. Ceux-ci sont gérés et configurés par la CNAF / CAF.</p> <ul style="list-style-type: none"> • Les collaborateurs du prestataire doivent respecter les règles mises en place par la CNAF / CAF ; • Les collaborateurs du prestataire n'ont pas les droits administrateurs sur les postes de la CNAF / CAF sauf sur autorisation formelle ; • Aucune application non validée par la CNAF / CAF ne peut être installée sur les postes de la CNAF / CAF sauf sur autorisation formelle ; • La configuration de base des postes de la CNAF / CAF ne doit pas être modifiée.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.5 CONTROLE D'ACCES

Objectif de ce chapitre : les processus de contrôle d'accès sont destinés à permettre la protection des informations et ressources et aident à partager les responsabilités.

8.5.1 EXIGENCES METIER EN MATIERE DE CONTROLE D'ACCES

Objectif : Limiter l'accès à l'information et aux moyens de traitement de l'information.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.1.1*	Obligatoire	Politique de contrôle d'accès. Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.	<ul style="list-style-type: none"> ▪ Fournit la politique de gestion des accès ▪ Valide les demandes d'accès. ▪ Met en place une séparation des rôles dans le processus de gestion des accès (demande, autorisation, administration) ▪ Fournit des listes des accès sur simple demande. ▪ Conserve les traces des demandes ou de modification d'accès 	<ul style="list-style-type: none"> ▪ Fournit les principes du respect du besoin d'en connaître. ▪ Décrit la cohérence entre les accès et la classification des informations / actifs ▪ Fournit les obligations légales et contractuelles pour la protection des données ou de services ▪ Décrit les profils / rôles ▪ Gère les comptes partagés ou génériques ▪ Définit la ségrégation des accès (demande, autorisation, administration) ▪ Effectue une revue périodique des accès ▪ Demande la suppression

			▪ Effectue une revue périodique des accès	des accès
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
9.1.1	Politique de contrôle d'accès. Revue périodique de validation de la politique.	Base annuelle
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.1.2	Obligatoire	Accès aux réseaux et aux services en réseau. Les utilisateurs ont uniquement accès au réseau et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation.	<ul style="list-style-type: none"> ▪ Fournit une politique d'accès au réseau et des services en réseau ▪ Sensibilise les intervenants sur les règles d'accès à la CNAF / CAF ▪ Met en place des procédures d'autorisation d'accès au réseau et services en réseau ▪ Surveille et contrôle l'utilisation du réseau et des services en réseau 	<ul style="list-style-type: none"> ▪ Fournit les principes d'accès au réseau et des services en réseau de la CNAF / CAF ▪ Met en place les restrictions d'accès au réseau et aux services en réseau ▪ Surveille et contrôle l'utilisation du réseau et des services en réseau
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				

8.5.2 GESTION DE L'ACCES UTILISATEUR

Objectif : Maitriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.2.1	Obligatoire	Enregistrement et désinscription des utilisateurs. Une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès est mise en œuvre.	<ul style="list-style-type: none"> Fournit une procédure de gestion des identifiants utilisateurs 	<ul style="list-style-type: none"> Fournit la liste des utilisateurs de la CNAF / CAF
<i>Exigence applicable par le prestataire</i> <div style="float: right;">OUI <input type="checkbox"/> NON <input type="checkbox"/></div>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.2.2*	Obligatoire	Maitriser la gestion des accès utilisateur. Un processus de maîtrise de la gestion des attributions ou des révocations des droits d'accès accordés à des identifiants utilisateurs inclue doit être mis en œuvre.	<ul style="list-style-type: none"> Fournit le processus de gestion des attributs des accès utilisateur Décrit le mécanisme de récupération des attributs des utilisateurs (Assertion SAML de préférence, ou solution proposée) Décrit la solution permettant la gestion des différents niveaux des attributs sur les différents composants (Outils de pilotage et d'évaluation, etc.) 	<ul style="list-style-type: none"> Définit et Fournit les attributs par profil utilisateur CNAF / CAF Fournit la liste des attributs des utilisateurs de la CNAF / CAF Fournit le paramétrage nécessaire en cas de récupération automatique des attributs
<i>Exigence applicable par le prestataire</i> <div style="float: right;">OUI <input type="checkbox"/> NON <input type="checkbox"/></div>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF

9.2.3	Obligatoire	Gestion des privilèges d'accès. L'attribution et l'utilisation des privilèges d'accès doivent être restreintes et contrôlées.	<ul style="list-style-type: none"> Fournit une procédure d'autorisation et de contrôle des accès à privilèges Identifie les privilèges associés à chaque système et processus Attribue les privilèges au juste droit Fournit la liste des intervenants du prestataire nécessitant des privilèges d'accès 	<ul style="list-style-type: none"> Fournit la liste des utilisateurs CNAF / CAF nécessitant des privilèges d'accès
-------	-------------	--	--	---

Exigence applicable par le prestataire

OUI ☐ NON ☐

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.2.4	Obligatoire	Gestion des informations secrètes d'authentification des utilisateurs. L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.	<ul style="list-style-type: none"> Communique de manière sécurisée les informations d'authentification temporaire unique par utilisateur Modifie les informations secrètes d'authentification par défaut définies dans les systèmes et logiciels 	<ul style="list-style-type: none"> Communique de manière sécurisée les informations d'authentification temporaire unique par utilisateur Modifie les informations secrètes d'authentification par défaut définies dans les systèmes et logiciels

Exigence applicable par le prestataire

OUI ☐ NON ☐

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.2.5	Obligatoire	Revue des droits d'accès utilisateur. Les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers.	<ul style="list-style-type: none"> Fournit une procédure de revue des droits d'accès des utilisateurs intervenant sur la solution Réalise, à minima annuellement, une revue des droits d'accès des utilisateurs intervenant sur la solution Corrige les anomalies détectées lors des revues 	<ul style="list-style-type: none"> Contrôle les résultats des revues

Exigence applicable par le prestataire	OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
9.2.2	Maitrise de la gestion des accès des utilisateurs	<p>Le prestataire doit proposer de préférence une authentification transparente (Single Sign On via le protocole SAML 2.0) sur sa solution pour les utilisateurs accédant depuis le réseau interne de la CNAF / CAF.</p> <p>A défaut de proposer une authentification transparente (Single Sign On), le prestataire doit mettre en œuvre un mécanisme d'authentification respectant la doctrine de la CNIL concernant l'authentification par mots de passe (Délibération n° 2022-100 du 21 juillet 2022).</p> <p>La solution doit permettre la gestion des différents niveaux d'accréditations, si possible via Assertion SAML, sur les différents composants (Outils de pilotage et d'évaluation, etc.).</p>

Exigence applicable par le prestataire	OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	
9.2.*	Gestion des accès des utilisateurs Les contrôles d'accès des utilisateurs du Prestataire sur ses systèmes sont de sa responsabilité.

Exigence applicable par le prestataire	OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	

8.5.3 RESPONSABILITES DES UTILISATEURS

Objectif : Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
--------------	---------	--------	-------------	------------

9.3.1*	Obligatoire	Utilisation d'informations secrètes d'authentification. Les utilisateurs des informations secrètes d'authentification doivent avoir une gestion responsable.	<ul style="list-style-type: none"> ▪ Sensibilise les intervenants du prestataire sur les règles de gestion des informations secrètes d'authentification ▪ Préviens la CNAF / CAF en cas de compromission des informations secrètes d'authentification ▪ Change les informations secrètes d'authentification en cas de compromission 	<ul style="list-style-type: none"> ▪ Préviens le prestataire en cas de compromission des informations secrètes d'authentification du prestataire
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
9.3.1	Responsabilité des utilisateurs	Les mesures relatives à la responsabilité des collaborateurs du prestataire sont de sa responsabilité.
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>		
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.5.4 CONTROLE DE L'ACCES AU SYSTEME ET AUX APPLICATIONS

Objectif : Empêcher les accès non autorisés aux systèmes et aux applications.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
9.4.1	Obligatoire	Restriction d'accès à l'information. L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.	<ul style="list-style-type: none"> ▪ Applique les mesures décrites dans 9.1.1 	<ul style="list-style-type: none"> ▪ Contrôle l'application des mesures décrites dans 9.1.1
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

9.4.2*	Obligatoire	Sécuriser les procédures de connexion. Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.	<ul style="list-style-type: none"> ▪ Implémenter et documenter les procédures de connexion sécurisée. ▪ Afficher une bannière avec la mire d'authentification sur les machines client et équipement réseau gérés par le prestataire (si techniquement possible). ▪ Afficher un message de connexion à propos de l'usage de l'actif après chaque authentification effective (si techniquement possible). 	<ul style="list-style-type: none"> ▪ Fournir les recommandations pour une connexion sécurisée.
--------	-------------	---	--	---

Exigence applicable par le prestataire

OUI ☐ NON ☐

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
9.4.2	Sécuriser les procédures de connexion.	<p>La procédure de connexion sécurisée doit inclure (non limitée à) :</p> <ul style="list-style-type: none"> ▪ Affichage d'avertissement, ▪ Nombre de connexions infructueuses, ▪ Délai entre des tentatives de connexions infructueuses, ▪ Chiffrer le mot de passe. <p>Bannière de connexion</p> <ul style="list-style-type: none"> ▪ Avant une connexion réussie, toutes les bannières sur les ordinateurs clients et les équipements de réseau gérés par Prestataire doivent demander à l'utilisateur de se connecter, en fournissant l'information de connexion comme requis. <p>Message Bannière</p> <ul style="list-style-type: none"> ▪ Quand une bannière est affichée, le message de la bannière doit être approuvé par la CNAF / CAF et par le Prestataire.

Exigence applicable par le prestataire

OUI ☐ NON ☐

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

9.4.3	Système de gestion des mots de passe	Le prestataire doit mettre en œuvre un système de gestion de mot de passe respectant la doctrine de la CNIL concernant l'authentification par mots de passe (Délibération n° 2022-100 du 21 juillet 2022).
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>		
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.6 CRYPTOGRAPHIE

Objectif général du Chapitre : assurer une utilisation correcte et efficace de la cryptographie pour protéger la confidentialité, l'authenticité et / ou l'intégrité de l'information.

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
10.1.*	Mesures Cryptographiques	<p>La gestion des clés cryptographiques utilisées pour la protection des données de la CNAF / CAF est de la responsabilité de la CNAF / CAF.</p> <p>Le prestataire doit mettre en œuvre une politique de gestion, de protection, d'utilisation et de durée de vie des clés cryptographiques. Il doit en outre :</p> <ul style="list-style-type: none"> Le prestataire doit avoir une gestion sécurisée des bi-clés nécessaire à l'établissement des connexions TLS (coffre-fort numérique). <p>Le prestataire doit intégrer les algorithmes et protocoles de chiffrement fournis par la CNAF / CAF</p>
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>		
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		
	Outils de chiffrement	Toutes les données dites sensibles selon la classification utilisée pour le contrat devront être chiffrées avant transmission. Les solutions utilisées doivent répondre aux exigences de la CNAF / CAF (7-ZIP, ou d'autres outils comme Prim'X ZED par exemple)
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>		
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.7 SECURITE PHYSIQUE ET ENVIRONNEMENTALE

Objectif de ce chapitre : Le contrôle de la sécurité physique et environnementale permettra d'éviter :

- Tout accès physique non autorisé.
- Des dommages et des intrusions dans les locaux,
- Des accès non autorisés aux informations de l'entreprise,
- La perte, les altérations, le vol ou la compromission des actifs,
- L'interruption d'activités de l'entreprise.

8.7.1 ZONES SECURISEES

Objectif : empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
11.1.*	Zones sécurisées	<p>Le prestataire identifie des périmètres de sécurité servant à protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information utilisés dans le cadre de la prestation</p> <p>Il protège les zones sécurisées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.</p> <p>Le prestataire applique des mesures de sécurité physique aux bureaux, aux salles et aux équipements contre les désastres naturels, les attaques malveillantes ou les accidents.</p> <p>Le prestataire applique des procédures pour le travail en zone sécurisée. Le personnel extérieur intervenant dans les zones sécurisés doit être accompagné tout au long de leur intervention.</p> <p>L'implémentation et la revue des mesures liées à la sécurisation des zones (Datacenter et bureau) et des équipements, selon les mesures de l'ISO, sont de la responsabilité du Prestataire.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p>Justification lorsque le prestataire juge la mesure non applicable.</p>		

8.7.2 MATERIELS

Objectif : Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
--------------	------------	----------------------------

11.2.*	Sécurisation des matériels	<p>Protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux</p> <p>Protéger les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information contre toute interception, interférence ou dommage.</p> <p>Appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.</p> <p>Vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.</p> <p>S'assurer que le matériel non surveillé est doté d'une protection appropriée</p> <p>Adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
11.2.*	Sécurisation des matériels	<p>Incluant un audit et/ou un test des installations (alimentation électrique, HVAC, UPS, groupe électrogène, etc.) sur une base annuelle.</p> <p>Une inspection physique des équipements non autorisés sur une base annuelle.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.8 SECURITE LIEE A L'EXPLOITATION

Objectif de ce chapitre : Pour assurer le fonctionnement correct et sûr des installations de traitement de l'information, il faut mettre en œuvre et maintenir le niveau approprié de sécurité de l'information et de services, réduire le risque de pannes des systèmes, protéger l'intégrité des logiciels et de l'information, empêcher la divulgation non autorisée, la modification, la suppression ou la destruction de biens.

8.8.1 PROCEDURES ET RESPONSABILITES LIEES A L'EXPLOITATION

Objectif : S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.1.1	Obligatoire	Procédures d'exploitation documentées. Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.	<ul style="list-style-type: none"> Documente et maintient des procédures utilisées dans le cadre de la prestation. Produit les procédures à la demande de la CNAF / CAF 	<ul style="list-style-type: none"> Fournit les éléments requis pour l'établissement des procédures. Fournit les calendriers requis (interdépendances avec les autres systèmes, plan batch avec heures de début et de fin des traitements)
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.</i>				
12.1.2	Obligatoire	Gestion des changements. Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.	<ul style="list-style-type: none"> Identifie et applique les mesures de sécurité dans le processus de changement Conserve les traces de tous les changements Planifie et teste les changements Évalue les impacts potentiels des changements Définit les procédures de communication Définit les procédures de retour arrière. Définit un processus de modification d'urgence pour la résolution d'un incident 	<ul style="list-style-type: none"> Approuve les procédures pour les changements si nécessaire.
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				
12.1.3	Obligatoire	Dimensionnement. L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.	<ul style="list-style-type: none"> Ajuste les éléments de supervision des systèmes Surveille les tendances dans l'utilisation Suit les performances Assure la planification des évolutions de dimensionnement 	<ul style="list-style-type: none"> Fournit les éléments de performance attendues
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				
12.1.4*	Obligatoire	Séparation des environnements de développement, de test et d'exploitation. Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.	<ul style="list-style-type: none"> Sépare chaque environnement Applique des profils d'utilisateurs différents entre les environnements Met en place les procédures de transfert sécurisé de données entre les environnements. N'autorise pas les copies des données de production sur les environnements de non-production sans autorisation expresse du RSSI de la CNAF / MSSI de la CAF. Sépare logiquement ou physiquement les environnements de la CNAF / CAF vis-à-vis des autres clients 	<ul style="list-style-type: none"> Définit les règles de ségrégation et de transfert entre les environnements. Définit les profils utilisateurs et la ségrégation des fonctions Définit les procédures de transfert des données entre les environnements.
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
--------------	------------	----------------------------

12.1.4	Séparation des environnements de développement, de test et d'exploitation	<p>Lorsque l'utilisation des données personnelles à des fins de test ne peut être évitée, une évaluation des risques doit être effectuée et des mesures de sécurité doivent être appliquées pour atténuer les risques.</p> <p>Aucune des données personnelles ne peut être copiée de la production à des environnements de test ou de développement sans l'accord expresse du RSSI de la CNAF / MSSI de la CAF.</p>
<i>Exigence applicable par le prestataire</i> <div>OUI <input type="checkbox"/> NON <input type="checkbox"/></div>		
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.8.2 PROTECTION CONTRE LES LOGICIELS ET CODES MALVEILLANT ET MOBILE

Objectif : Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.

Chapitre ISO	Service	Mesure	Prestataire	CNAF
12.2.1*	Obligatoire	Mesures contre les logiciels malveillants. Des mesures de détection, de prévention et de récupération, conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.	<ul style="list-style-type: none"> Met en place une solution de protection contre les codes malveillants sur les machines du Prestataire Installe et met à jour la solution Assure la gestion de la solution (suivi du parc, scans des machines et des fichiers, mises à jour des signatures, reporting) Assure le maintien en condition de sécurité des logiciels et des équipements. Définit et gère les procédures d'alerte et de recouvrement en cas d'attaque. 	<ul style="list-style-type: none"> Met en place une politique permettant l'utilisation des seuls logiciels autorisés Met en place une politique pour obtenir des fichiers ou des logiciels autorisés (à partir du réseau ou supports externes) Pilote la gestion de crise Fournit les politiques de filtrage.
<i>Exigence applicable par le prestataire</i> <div>OUI <input type="checkbox"/> NON <input type="checkbox"/></div>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
--------------	------------	----------------------------

12.2.1	Mesures contre les logiciels malveillants.	Mise à jour des signatures journaliers ou au fil de l'eau (poste de travail, serveurs). Recherches de virus : Selon la configuration des serveurs et des contraintes applicatives : au fil de l'eau (I/O sur disques), Journalier (quick scan), Hebdomadaire (full)
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		
12.2.1	Mesures contre les logiciels malveillants. Mesures de détection et de prévention sur les postes de travail et terminaux mobiles.	Il convient d'appliquer les mesures décrites dans le chapitrage ISO 6.2.* sur les appareils mobiles et le télétravail
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.8.3 SAUVEGARDE

Objectif : Se protéger de la perte de données.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.3.1	Obligatoire	Sauvegarde des informations. Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisées et testées régulièrement conformément à une politique de sauvegarde convenue.	<ul style="list-style-type: none"> Formalise et met en œuvre une solution de sauvegarde et de restauration conformément aux exigences de la CNAF / CAF. Si la prestation le nécessite et si la CNAF / CAF le demande, met en œuvre une solution de chiffrement des sauvegardes. Teste la solution sauvegarde / restauration à minima annuellement. 	<ul style="list-style-type: none"> Définit la politique de sauvegarde et de restauration. Définit la période de rétention et d'archivage
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

8.8.4 JOURNALISATION ET SURVEILLANCE

Objectif : Enregistrer les événements et générer des preuves.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.4.1*	Obligatoire	Journalisation des événements. Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.	<ul style="list-style-type: none"> Mets en œuvre une politique de gestion des traces. 	<ul style="list-style-type: none"> Fournit le détail des logs d'audit qui doivent être ajoutée à la configuration standard.
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

12.4.2*	Obligatoire	Protection de l'information Journalisée. Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé.	<ul style="list-style-type: none"> Centralise les logs dans un système sécurisé Externalise et chiffre les logs de connexion et d'audits 	<ul style="list-style-type: none"> Fournit les éléments des logs d'audit qui doivent être externalisés et chiffrés
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				
12.4.3*	Obligatoire	Journaux administrateur et opérateur. Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.	<ul style="list-style-type: none"> Conserve les logs des journaux des activités des administrateurs et opérateurs 	<ul style="list-style-type: none"> Fournit les éléments qui doivent être journalisés.
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				
12.4.4	Obligatoire	Synchronisation des horloges. Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.	<ul style="list-style-type: none"> Fournit la méthode utilisée pour obtenir une heure de référence à partir d'une source externe et la méthode utilisée pour synchroniser de manière fiable les horloges internes <ul style="list-style-type: none"> Garantit la précision de journaux d'audit (enquête, investigation) 	<ul style="list-style-type: none"> Pas d'action
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
12.4.1	Journalisation des événements.	<ul style="list-style-type: none"> En analysant les journaux d'audit, le prestataire garantit que la CNAF / CAF ne peut accéder qu'aux dossiers qui se rapportent qu'à ses activités. Un autre client du prestataire ne doit pas pouvoir accéder aux enregistrements qui se

		<p>rapportent aux activités de la CNAF / CAF.</p> <ul style="list-style-type: none"> Le prestataire réalise une analyse régulière des journaux d'audit à la recherche d'évènements pouvant présenter un risque pour la sécurité des données. Si la CNAF / CAF le demande et que la solution le permet, les traces doivent pouvoir être injecter dans notre solution SIEM.
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
12.4.2	Protection de l'information Journalisée.	<ul style="list-style-type: none"> Les informations enregistrées pour la surveillance de la sécurité et du diagnostic opérationnel peuvent contenir des données personnelles. Des mesures telles que le contrôle d'accès (Chapitre 9.2 ISO), doivent être mises en place pour garantir que les informations consignées sont utilisées uniquement aux fins prévues. Des revues régulières des droits d'accès aux journaux d'audit doivent être mis en place Une procédure doit être mise en place pour assurer que les informations enregistrées sont supprimées dans un délai déterminé et documenté, validé avec la CNAF / CAF
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
12.4.3	Journaux administrateur et opérateur.	<p>Les informations qui doivent être enregistrées (sans s'y limiter) :</p> <ul style="list-style-type: none"> Compte utilisé, Processus impliqué, Date / heure, Information (dossier traité, processus lancé) ou l'échec
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.8.5 MAITRISE DES LOGICIELS EN EXPLOITATION

Objectif : Garantir l'intégrité des systèmes en exploitation.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.5.1	Obligatoire	Gestion des logiciels en exploitation. Les informations sur les	<ul style="list-style-type: none"> Maintient à jour la CMDB ou la liste des outils et/ou des logiciels présents sur 	<ul style="list-style-type: none"> Fournit, si nécessaire, la liste des logiciels préconisés.

		logiciels constituant les systèmes d'information en exploitation doivent être maintenues à jour sans délai (Procédure de maintien en conditions opérationnelles)	les systèmes gérés par le Prestataire. ▪ Fournit une procédure de maintien en conditions opérationnelles	
Exigence applicable par le prestataire				
OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				

8.8.6 GESTION DES VULNERABILITES TECHNIQUES

Objectif : Empêcher toute exploitation des vulnérabilités techniques.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.6.1*	Obligatoire	Gestion des vulnérabilités techniques. Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé	<ul style="list-style-type: none"> ▪ Rédige et applique une procédure de maintien en condition de sécurité ▪ Identifie, analyse et propose des correctifs de sécurité selon la criticité, les impacts relatifs à l'environnement de la CNAF / CAF : plan de correction ▪ Déploie et valide les correctifs sur le système en environnement de validation avant tout déploiement en production ▪ Procède au retour arrière si nécessaire 	<ul style="list-style-type: none"> ▪ Évalue la gravité en fonction des risques ▪ Valide le plan de correction ▪ Valide les correctifs proposés, et demande à appliquer des tests de non-régression
Exigence applicable par le prestataire				
OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				
12.6.2	Obligatoire	Restrictions liées à l'installation de logiciels. Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.	<ul style="list-style-type: none"> ▪ Implémente les restrictions pour être conforme aux règles établies. 	<ul style="list-style-type: none"> ▪ Fournit, si nécessaire, la liste des logiciels autorisés.

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.8.7 CONSIDERATIONS SUR L'AUDIT DES SYSTEMES D'INFORMATION

Objectif : Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
12.7.1*	Obligatoire	Mesures relatives à l'audit des systèmes d'information. Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.	<ul style="list-style-type: none"> Autorise après validation le périmètre des audits Donne les accès en lecture sur les systèmes qu'ils utilisent pour réaliser la prestation (accès aux logs, à la supervision et à la documentation) Documente les procédures, les exigences et les responsabilités 	<ul style="list-style-type: none"> Définit ses exigences d'audit, le périmètre, les objectifs, les ressources. Informe le prestataire dans un délai raisonnable avant la réalisation de l'audit

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
12.7.1	Mesures relatives à l'audit des systèmes d'information	Le prestataire accepte formellement que la CNAF / CAF ou un mandataire puisse réaliser des audits de sécurité sur la solution mise à disposition dans le cadre de la prestation.

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
--------------	------------	----------------------------

12.6.1	Gestion des vulnérabilités techniques	<p>L'identification des correctifs et l'analyse suit le calendrier de l'éditeur (sur une base régulière ou sur alerte). Ces délais peuvent être plus courts en cas d'injonction.</p> <p>Proposer un plan de correction :</p> <ul style="list-style-type: none"> ▪ Pour les correctifs hautement critiques : Dans les 2 jours après la sortie du correctif ▪ Pour les correctifs à criticité moyenne : Dans les 7 jours après la sortie du correctif ▪ Pour les correctifs à criticité basse : Dans les 15 jours après la sortie du correctif <p>Les commentaires des clients (acceptation ou refus pour l'installation) doivent être obtenus au moins 1 jour avant la date de déploiement prévue.</p> <p>Déploiement des correctifs :</p> <ul style="list-style-type: none"> ▪ Pour les correctifs hautement critiques : 5 jours ouvrés suivants la sortie du correctif ▪ Pour les correctifs à criticité moyenne : 15 jours ouvrés suivants la sortie du correctif ▪ Pour les correctifs à criticité basse : 30 jours ouvrés après la sortie du correctif
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.9 SECURITE DES COMMUNICATIONS

Objectif de ce chapitre :

Assurer les communications entre les services, entre les réseaux et lors des transferts d'information :

- Fixer et maintenir un niveau de sécurité approprié de l'information et de son service,
- Maintenir l'intégrité, la disponibilité et la sécurité de l'information échangés entre la CNAF / CAF et le prestataire et toute entité externe,
- Détecter des activités non autorisées.

8.9.1 MANAGEMENT DE LA SECURITE DES RESEAUX

Objectif : Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
13.1.1*	Obligatoire	Contrôle des réseaux. Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les	<ul style="list-style-type: none"> ▪ Documente et maintient les spécifications et design du réseau, les procédures 	<ul style="list-style-type: none"> ▪ Définit la responsabilité opérationnelle pour préserver la disponibilité, la confidentialité et

		<p>systèmes et les applications.</p>	<p>opérationnelles</p> <ul style="list-style-type: none"> ▪ Teste les procédures opérationnelles mise en place ▪ Établit les responsabilités et procédures pour la gestion des équipements pour les accès distants y compris pour les utilisateurs. ▪ Sépare les responsabilités opérationnelles du réseau vis à vis de la gestion des ordinateurs ▪ Configure des mesures spécifiques pour garantir la confidentialité et l'intégrité des données transitant sur le réseau public et vers les systèmes connectés. ▪ Gère les activités pour optimiser les services et assure que les mesures sont appliquées efficacement dans toute l'infrastructure. ▪ Trace et supervise les actions 	<p>l'intégrité des données</p>
<p>Exigence applicable par le prestataire</p> <p>OUI <input type="checkbox"/> NON <input type="checkbox"/></p>				
<p>Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				
13.1.2	Obligatoire	<p>Sécurité des services de réseau. Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.</p>	<ul style="list-style-type: none"> ▪ Réalise une analyse de risque liée aux infrastructures réseau mise à disposition dans le cadre de la prestation ▪ Fournit la documentation, les tableaux de bord, le reporting relative à la gestion du réseau. ▪ Implémente le filtrage IP sur les adresses publiques CNAF en cas d'utilisation d'internet ▪ Implémente si nécessaire une liaison VPN site à site 	<ul style="list-style-type: none"> ▪ Fournit les caractéristiques de l'interconnexion réseau souhaité pour la prestation ▪ Vérifie la conformité au SLA ▪ Revoie le contenu des tableaux de bord et des rapports ▪ Analyse les tableaux de bord et les rapports
<p>Exigence applicable par le prestataire</p> <p>OUI <input type="checkbox"/> NON <input type="checkbox"/></p>				

<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
13.1.3	Obligatoire	Cloisonnement des réseaux. Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux.	<ul style="list-style-type: none"> Implémente les zones cloisonnées 	<ul style="list-style-type: none"> Définit les zones selon les applications métiers, le regroupement des serveurs, la sensibilité des informations, etc.
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
13.1.1	Contrôle des réseaux	La responsabilité du prestataire ne s'entend pas aux équipements réseau gérés par la CNAF / CAF (routeurs, switches, IDS, firewalls, etc.).
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.9.2 TRANSFERT DE L'INFORMATION

Objectif : Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
13.2.1*	Obligatoire	Politiques et procédures de transfert de l'information. Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.	<ul style="list-style-type: none"> Applique l'ensemble des politiques et procédures pour protéger les transferts d'information 	<ul style="list-style-type: none"> Pas d'action
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire.</i>				

Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
13.2.2*	Obligatoire	Accords en matière de transfert d'information. Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.	<ul style="list-style-type: none"> Utilise des applications et procédures spécifiques pour protéger les informations sensibles. Possède des procédures pour la création et le partage des clés de chiffrement. 	<ul style="list-style-type: none"> Fournit la politique de transfert de l'information entre la CNAF / CAF et le Prestataire
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
13.2.4	Obligatoire	Engagements de confidentialité ou de non-divulgence. Les exigences en matière d'engagements de confidentialité ou de non-divulgence, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins.	<ul style="list-style-type: none"> Maintient sa politique relative à la confidentialité et ses accords de non-divulgence (NDA). Fournit sur demande sa politique relative à la confidentialité et les accords de non-divulgence (NDA). 	<ul style="list-style-type: none"> Fournit / valide les accords de confidentialité et de non-divulgence (NDA) Revoit les accords à minima annuellement
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
Description des mesures de sécurité mises en œuvre par le prestataire <i>lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
13.2.1	Politiques et procédures de transfert de l'information	<p>Chaque fois que les médias physiques sont utilisés pour le transfert de l'information, un système doit être mis en place pour enregistrer les médias physiques entrants et sortants contenant des données personnelles (type et la référence de médias physiques, l'expéditeur / destinataires autorisés, la date et l'heure).</p> <p>La CNAF / CAF peut demander la mise en place de mesures supplémentaires (telles que le chiffrement) pour assurer que les données ne peuvent être consultées ni sur le point de destination, ni durant le trajet.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.		
Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
13.2.2	Accords en matière de transfert d'information	<p>Les échanges de données en mode transfert de fichiers s'effectuent via la plate-forme d'échange centralisée et automatisée de la CNAF / CAF conformément aux règles de sécurité :</p> <ul style="list-style-type: none"> Tous les échanges sont chiffrés au travers du protocole TLS 1.2 à minima Tous les flux sont chiffrés entre le navigateur client et le serveur ou le cas échéant, entre les serveurs (flux webservice, SOAP, SAML, etc...) <p>Le soumissionnaire indique dans sa réponse technique la solution proposée pour le transfert de fichiers. Les protocoles admissibles sont PESIT ou PESIT utilisant SSL de préférence voire SFTP.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.		

8.10 ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION

8.10.1 EXIGENCES DE SECURITE APPLICABLES AUX SYSTEMES D'INFORMATION

Objectif : Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
14.1.3	Obligatoire	Protection des transactions liées aux services d'application. L'information impliquée dans les transactions liées aux services d'application pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa	<ul style="list-style-type: none"> Chiffrer le ou les canaux de communications entre toutes les parties impliquées Sécuriser les protocoles utilisés entre toutes les parties impliquées Sécuriser le processus de gestion des certificats et signatures 	<ul style="list-style-type: none"> Fournit des exigences de protocoles à utiliser et de gestion des certificats et signatures Fournit des paramètres nécessaires à l'établissement du ou des canaux de communication Fournit les certificats nécessaires dans le cadre de la prestation

		réémission doit être protégée.		
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

8.10.2 SECURITE DES PROCESSUS DE DEVELOPPEMENT ET D'ASSISTANCE TECHNIQUE

Objectif : S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
14.2.1	Obligatoire	Politique de développement sécurisé. Des règles de développement des logiciels et des systèmes sont établies et appliquées aux développements de l'organisation	<ul style="list-style-type: none"> ▪ Définit la politique de développement sécurisé et la fait appliquer ▪ Sensibilise régulièrement ses équipes aux bonnes pratiques de développement (OWASP, etc.) 	<ul style="list-style-type: none"> ▪ Définit la politique de développement sécurisé et la fait appliquer ▪ Contrôle que la sensibilisation est effective
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
14.2.2	Obligatoire	Procédures de contrôle des changements apportés au système. Les changements apportés au système dans le cycle de développement doivent être contrôlés en utilisant des procédures formelles de contrôle des changements	<ul style="list-style-type: none"> ▪ Définit et applique les procédures de contrôles des changements ▪ Planifie les contrôles 	<ul style="list-style-type: none"> ▪ Définit les procédures de contrôles des changements ▪ Planifie et analyse les résultats des contrôles
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

14.2.6*	Obligatoire	Environnement de développement sécurisé. Un environnement de développement sécurisé est mis en place pour les tâches de développement et d'intégration du système qui englobe l'intégralité du cycle de développement du système	<ul style="list-style-type: none"> ▪ Met en place l'environnement sécurisé ▪ N'utilise que des données fictives 	<ul style="list-style-type: none"> ▪ Contrôle les éléments de sécurité mis en œuvre
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
14.2.8	Obligatoire	Phase de test de la sécurité du système. Des tests des fonctionnalités de sécurité doivent être réalisés pendant le développement	<ul style="list-style-type: none"> ▪ Réalise les tests 	<ul style="list-style-type: none"> ▪ Contrôle les résultats des tests et audit les développements avant réception
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
14.2.9	Obligatoire	Test de conformité du système. Les programmes de test de conformité et des critères associés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions doivent être déterminés et appliqués	<ul style="list-style-type: none"> ▪ Définit les critères de conformité ▪ Utilise des outils d'analyse de codes ou des scanners de vulnérabilité ▪ Vérifie les actions correctives apportées au défaut lié à la sécurité 	<ul style="list-style-type: none"> ▪ Conseille l'utilisation du standard ouvert OWASP, NIST, etc
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
--------------	------------	----------------------------

14.2.6	Environnement de développement	<p>Il est de la responsabilité du prestataire de fournir des postes de travail sécurisés à ses équipes lorsqu'ils ne sont pas fournis par la CNAF / CAF.</p> <p>Il est nécessaire d'appliquer la mesure 12.2.1 décrit au chapitre 8.8.2 de ce document</p>
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>		
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.10.3 DONNEES DE TEST

Objectif : Garantir la protection des données utilisées pour les tests.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
14.3.1	Obligatoire	Protection des données de test. Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.	<ul style="list-style-type: none"> ▪ Demande la fourniture de données fictives à la CNAF / CAF ou produit des données fictives ▪ Demande l'autorisation chaque fois qu'une information d'exploitation doit être copié dans un environnement hors production ▪ Produit un certificat de destruction dès que le jeu de données n'est plus utile dans le cas d'utilisation de données d'exploitation. 	<ul style="list-style-type: none"> ▪ Fournit les données ▪ Définit et contrôle leur cycle de vie. ▪ Exige le certificat de destruction dans le cas d'utilisation de données d'exploitation
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>				

8.11 GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

8.11.1 GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION ET AMELIORATIONS

Objectif : Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
16.1.1*	Obligatoire	Responsabilités et procédures. Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information doivent être établies.	<ul style="list-style-type: none"> ▪ Définit et applique des procédures de gestion des incidents liés à la sécurité de l'information ▪ Communique vers la CNAF / CAF tout incident dans les plus bref délai (48 h) 	<ul style="list-style-type: none"> ▪ Valide les procédures de gestion des incidents de sécurité
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.2	Obligatoire	Signalement des événements liés à la sécurité de l'information. Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.	<ul style="list-style-type: none"> ▪ Signale les incidents de sécurité au RSSI de la CNAF / MSSI de la CAF et à la liste des contacts fournie. ▪ Nomme des points de contacts 	<ul style="list-style-type: none"> ▪ Fournit une liste de contacts
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.3	Obligatoire	Signalement des failles liées à la sécurité de l'information. Les salariés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	<ul style="list-style-type: none"> ▪ Voir la mesure 16.1.2 	<ul style="list-style-type: none"> ▪ Voir la mesure 16.1.2
<i>Exigence applicable par le prestataire</i> OUI <input type="checkbox"/> NON <input type="checkbox"/>				
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.4	Obligatoire	Appréciation des événements liés à la sécurité de l'information et prise de décision. Les événements liés à la sécurité de l'information	<ul style="list-style-type: none"> ▪ Définit l'échelle de classification des incidents de sécurité ▪ Enregistre les conclusions de 	<ul style="list-style-type: none"> ▪ Valide l'échelle de classification proposée

		doivent être appréciés, classés comme incidents liés à la sécurité de l'information au besoin.	l'appréciation et la décision	
<i>Exigence applicable par le prestataire</i>			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.5	Obligatoire	Réponse aux incidents liés à la sécurité de l'information. Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.	<ul style="list-style-type: none"> Fournit les procédures 	<ul style="list-style-type: none"> Valide les procédures
<i>Exigence applicable par le prestataire</i>			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.6	Obligatoire	Tirer des enseignements des incidents liés à la sécurité de l'information. Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.	<ul style="list-style-type: none"> Rédige un RETEX suite à chaque incident de sécurité 	<ul style="list-style-type: none"> Participe au RETEX impliquant les actifs de la CNAF / CAF
<i>Exigence applicable par le prestataire</i>			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
16.1.7*	Obligatoire	Recueil de preuves. L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.	<ul style="list-style-type: none"> Rédige et applique des procédures de recueil et de traitement des preuves Conserve et protège les éléments relatifs à tous les incidents de sécurité comme requis par la loi Conserve et protège tous les éléments de recherche d'information, le détail et les résultats de chaque incident de sécurité 	<ul style="list-style-type: none"> Demande les éléments de preuves afin de répondre à des exigences réglementaires Fournit des experts avec les accès requis pour collecter et conserver les preuves relatives à l'incident de sécurité si besoin.

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
16.1.1	Responsabilités et procédures.	<p>Pour un incident suspecté d'avoir été initié à partir des équipements de la CNAF / CAF et impactant les équipements ou les infrastructures du Prestataire ou d'un autre client, la CNAF / CAF doit collaborer avec le Prestataire pour résoudre l'incident et prendre les mesures nécessaires pour veiller à ce que de tels incidents ne se reproduisent pas.</p> <p>Pour la réponse aux incidents de sécurité du Prestataire, le Prestataire gère ceux-ci selon ses procédures et sa politique.</p>

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
16.1.7	Collecte de preuves.	<p>Le Prestataire fournira à la CNAF / CAF et sur demande du RSSI de la CNAF / MSSI de la CAF, en cas de besoin, une assistance sur place au sein des sites de la CNAF / CAF pour permettre l'analyse et la collecte.</p>

Exigence applicable par le prestataire	OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.12 ASPECTS DE LA SECURITE DE L'INFORMATION DANS LA GESTION DE LA CONTINUITE DE L'ACTIVITE

Objectif de ce chapitre : L'organisation, la planification, la mise en œuvre, la vérification, la révision et l'évaluation est destinée à permettre de poursuivre les activités les plus critiques en cas de sinistre entraînant une indisponibilité du système d'information.

8.12.1 CONTINUITE DE LA SECURITE DE L'INFORMATION

Objectif : la continuité de la sécurité de l'information doit faire partie intégrante des systèmes de gestion de la continuité de l'activité

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
17.1.1*	Obligatoire	Organisation de la continuité de la sécurité de l'information. Les exigences en matière de sécurité de l'information et de continuité du management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre sont déterminés par l'organisation	<ul style="list-style-type: none"> Met en place une organisation pour assurer la continuité de la sécurité du système d'information Analyse l'impact sur l'activité 	<ul style="list-style-type: none"> Fournit les exigences de la CNAF / CAF
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				
Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
17.1.2	Obligatoire	Mise en œuvre de la continuité de la sécurité de l'information. L'organisation établit, documente, met en œuvre et maintient à jour des processus, des procédures et des mesures permettant de garantir le niveau requis de continuité de la sécurité de l'information au cours d'une situation défavorable	<ul style="list-style-type: none"> Définit des procédures de gestion de la continuité de l'activité Communique à la CNAF / CAF les procédures mise en œuvre 	<ul style="list-style-type: none"> Valide les procédures
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				
Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
17.1.3	Obligatoire	Vérifier, revoir et évaluer la continuité de la sécurité de l'information. L'organisation vérifie à intervalles réguliers les mesures de continuité de la sécurité de l'information déterminées et mises en œuvre, afin de s'assurer qu'elles restent valables et efficaces dans des situations défavorables.	<ul style="list-style-type: none"> Teste les procédures de gestion de la continuité de l'activité Communique à la CNAF / CAF les résultats Planifie des RETEX Revoit les procédures si nécessaire 	<ul style="list-style-type: none"> Participe aux tests de reprise d'activité Participe aux RETEX
Exigence applicable par le prestataire OUI <input type="checkbox"/> NON <input type="checkbox"/>				

*Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.*

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
17.1.1	Continuité de la sécurité de l'information	Il est de la responsabilité du Prestataire de gérer les mesures relatives à la continuité de la sécurité de l'information selon les chapitres de l'ISO Les tests de la continuité d'activité doivent être menés annuellement avec l'aval de la CNAF / CAF
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.</i>		

8.12.2 REDONDANCE

Objectif : Garantir la disponibilité des moyens de traitement de l'information.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
17.2.1*	Optionnel	Disponibilité des moyens de traitements de l'information. Des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité doivent être mis en œuvre	<ul style="list-style-type: none">▪ Etudie la nécessité de composant et/ou d'architecture redondante▪ Teste les systèmes d'information redondants	<ul style="list-style-type: none">▪ Pas d'action
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée. Justification lorsque le prestataire juge la mesure non applicable.				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
17.2.1	Disponibilité des moyens de traitement de l'information	Il est de la responsabilité du Prestataire de gérer les mesures relatives à la continuité de la sécurité de l'information selon les chapitres de l'ISO
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>

Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.
Justification lorsque le prestataire juge la mesure non applicable.

8.13 CONFORMITE

8.13.1 CONFORMITE AUX OBLIGATIONS LEGALES ET REGLEMENTAIRES

Objectif : Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
18.1.1*	Obligatoire	Identification de la législation et des exigences contractuelles applicables. Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisation elle-même.	<ul style="list-style-type: none"> Identifie les lois et règlements applicables selon les spécifications locales. Définit et documente les mesures spécifiques et les responsabilités. 	<ul style="list-style-type: none"> Identifie les lois et règlements applicables selon les spécifications locales.
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.1.2*	Obligatoire	Droits de propriété intellectuelle. Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.	<ul style="list-style-type: none"> Protège les biens qui sont sous propriété intellectuelle de la CNAF / CAF. 	<ul style="list-style-type: none"> Identifie les biens qui sont considérés comme couverts par la protection intellectuelle et les accords contractuels.
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.1.3	Obligatoire	Protection des enregistrements. Les enregistrements doivent être protégés de la perte, de la	<ul style="list-style-type: none"> Protège contre la détérioration des enregistrements. 	<ul style="list-style-type: none"> Fournit la durée de conservation de tous les

		destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.	<ul style="list-style-type: none"> Garantit les accès aux données (à la fois pour les supports et les lecteurs) durant une durée raisonnable. 	enregistrements. <ul style="list-style-type: none"> Fournit les spécifications pour l'archivage (dont le légal)
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.1.4	Obligatoire	Protection de la vie privée et protection des données à caractère personnel. La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation, les réglementations applicables et les clauses contractuelles le cas échéant.	<ul style="list-style-type: none"> Désigne un Délégué à la Protection des Données Maintient les règles de collecte des données, du traitement et la restriction dans la capacité de transférer des données à d'autres pays. 	<ul style="list-style-type: none"> Désigne un Délégué à la Protection des Données Définit les règles concernant les données à caractère personnel contre les collectes, traitement ou divulgation.
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.1.5	Obligatoire	Réglementation relative aux mesures cryptographiques. Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables.	<ul style="list-style-type: none"> Respecte les restrictions d'import et / ou d'export de matériels et logiciels relatifs à l'exécution des fonctions cryptographiques selon les réglementations applicables. Respecte les restrictions d'utilisation du chiffrement selon les réglementations applicables. 	<ul style="list-style-type: none"> Pas d'action
Exigence applicable par le prestataire			OUI <input type="checkbox"/> NON <input type="checkbox"/>	
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences de la CNAF / CAF
18.1.1	Identification de la législation et des exigences contractuelles applicables.	Les données à caractère personnel doivent être hébergées au sein de l'Union Européenne.
<i>Exigence applicable par le prestataire</i>		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		
18.1.2	Droits de propriété intellectuelle	<p>La propriété intellectuelle concerne (sans s'y limiter) :</p> <ul style="list-style-type: none"> ▪ L'acquisition du logiciel, ▪ La propriété des licences, ▪ Le nombre maximum d'utilisateurs, ▪ Les films, audio, photos, ▪ Les modes d'emploi, des livres, etc. ▪ Les preuves, ▪ La gestion d'actifs, ▪ Les procédures de transfert ou de suppression ▪ L'usage d'actif / système / logiciel / licence / vérification de données
<i>Exigence applicable par le prestataire</i>		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>		

8.13.2 REVUE DE LA SECURITE DE L'INFORMATION

Objectif : Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

Chapitre ISO	Service	Mesure	Prestataire	CNAF / CAF
18.2.1*	Obligatoire	Revue indépendante de la sécurité de l'information. Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.	<ul style="list-style-type: none"> ▪ Demande des ressources internes ou externes (sous contrat) pour évaluer la mise en œuvre de la gouvernance de la sécurité de l'information ▪ Fournit le résultat synthétique de la revue de la gouvernance de la sécurité de l'information 	<ul style="list-style-type: none"> ▪ Etudie les résultats de la gouvernance de sécurité dans le cadre de la prestation et propose un plan d'action (si nécessaire)
<i>Exigence applicable par le prestataire</i>			OUI <input type="checkbox"/> NON <input type="checkbox"/>	

<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.2.2	Obligatoire	Conformité avec les politiques et les normes de sécurité. Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.	<ul style="list-style-type: none"> Effectue une analyse d'écart entre la politique de sécurité et l'état de la sécurité Évalue les risques et les plans de correction suite aux écarts constatés. Initie le processus de gestion du changement pour les mesures de correction nécessaires. 	<ul style="list-style-type: none"> Approuve les demandes de changement, exécutées par le prestataire, pour la mise en œuvre de correction.
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				
18.2.3*	Obligatoire	Examen de la conformité technique. Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.	<ul style="list-style-type: none"> Planifie et documente les tests d'intrusion et de recherche de vulnérabilité. Définit des procédures, des outils et des exigences techniques Fournit un rapport d'évaluation (service spécifique) Met en place la gestion de la conformité des systèmes par rapport à la politique. 	<ul style="list-style-type: none"> Valide les processus de contrôle de conformité Définit les plannings avec le prestataire Valide les rapports d'évaluation
Exigence applicable par le prestataire			OUI <input type="checkbox"/>	NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>				

Chapitre ISO	Paramètres	Exigences DE LA CNAF / CAF
18.2.1	Revue indépendante de la sécurité de l'information.	L'examen du niveau de la sécurité de l'information est effectué sur une base régulière (à minima annuelle).

Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		
18.2.3	Vérification de la conformité technique, test d'intrusion ou recherché de vulnérabilités	<p>Toute brique SI livrée par le prestataire pourra faire l'objet d'un test d'intrusion ou d'une recherche de vulnérabilité par la CNAF / CAF ou un mandataire.</p> <p>La CNAF / CAF fournira une liste détaillée des vulnérabilités trouvées au prestataire.</p> <p>La correction des failles de sécurité devra être réalisée dans un délai fourni par la CNAF / CAF en fonction de la criticité des failles ou vulnérabilités identifiées.</p> <p>Le prestataire implémente les actions de correction (processus de gestion du changement) après validation de la CNAF / CAF.</p>
Exigence applicable par le prestataire		OUI <input type="checkbox"/> NON <input type="checkbox"/>
<i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i> <i>Justification lorsque le prestataire juge la mesure non applicable.</i>		

9. MESURES COMPLEMENTAIRES A L'ISO 27002

9.1 UTILISATION DE L'INTELLIGENCE ARTIFICIELLE (IA)

9.1.1 INTERDICTION DE L'USAGE DE L'IA

Chapitre ISO	Paramètres	Exigences DE LA CNAF / CAF
	Interdiction de l'usage de l'IA.	<p>Le prestataire s'engage à ne pas utiliser d'outils, de logiciels ou de services basés sur l'intelligence artificielle (IA) pour l'accomplissement des prestations définies dans le cadre de la prestation, sauf autorisation écrite express et préalable de la CNAF.</p> <p>Cette interdiction concerne notamment, mais sans s'y limiter :</p> <ul style="list-style-type: none"> • La création, la modification, le traitement ou l'analyse de documents, de données ou d'informations appartenant à la CNAF / CAF ; • L'automatisation de tâches techniques, organisationnelles ou décisionnelles relevant du périmètre contractuel ; • Toute autre activité pouvant affecter la sécurité, la confidentialité ou l'intégrité des informations traitées dans le cadre de la prestation. <p>La CNAF / CAF se réserve par ailleurs le droit de résilier le présent accord-cadre en cas de manquement à l'obligation définie ci-dessus, ce manquement constituant une faute particulièrement grave.</p>

Exigence applicable par le prestataire	OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	

9.1.2 DEMANDE D'AUTORISATION DE L'USAGE DE L'IA

Chapitre ISO	Paramètres	Exigences DE LA CNAF / CAF
	<p>Demande d'autorisation formelle de l'usage de l'IA.</p>	<p>En cas de demande d'autorisation d'utilisation de l'IA, le prestataire devra formuler par écrit une demande à la CNAF / CAF contenant une description détaillée de l'outil d'IA envisagé. Cette demande doit inclure une évaluation des risques menée par le prestataire et validée par la CNAF / CAF. Cette évaluation devra notamment porter sur :</p> <ul style="list-style-type: none"> • La finalité d'utilisation ; • Ses fonctionnalités principales ; • Les données traitées par l'IA ; • Les technologies ou systèmes d'IA envisagés ; • Les garanties offertes en termes de sécurité, confidentialité et protection des données, notamment en ce qui concerne l'entraînement des modèles et le stockage des données ; • Les risques potentiels identifiés et les mesures d'atténuation associées. <p>La solution envisagée devra respecter également la « Politique Nationale de sécurité d'utilisation de l'IA ».</p> <p>De plus, si la prestation implique le traitement de données à caractère personnel ou sensible, le prestataire réalise une analyse d'impact relative à la protection des données (DPIA).</p> <p>La CNAF / CAF se réserve par ailleurs le droit de résilier le présent accord-cadre en cas de manquement à l'obligation définie ci-dessus, ce manquement constituant une faute particulièrement grave.</p>

Exigence applicable par le prestataire	OUI <input type="checkbox"/> NON <input type="checkbox"/>
<p><i>Description des mesures de sécurité mises en œuvre par le prestataire lorsque la mesure est appliquée.</i></p> <p><i>Justification lorsque le prestataire juge la mesure non applicable.</i></p>	