



**l'Assurance
Maladie**

BOUCHES-DU-RHÔNE



Livret de sécurité du prestataire

La sécurité de l'information nous concerne tous

932-SSI - PUBLIC - CPCAM131

Sommaire

Accès aux sites	p.4
Accès aux locaux	p.5
Confidentialité	p.6
Prise en compte des principes de protection des données	p.7
Accès au Système d'Information	p.8-9
Accès à distance au Système d'Information	p.10-11
Remontées d'incidents	p.12
Fin de prestation	p.13
Sanctions applicables	p.14
Référents - Contacts	p.15

Introduction

Votre société s'est engagée, par contrat, à faire respecter par ses salariés, et éventuels sous-traitants, les mesures de sécurité et de confidentialité applicables dans les locaux et sur le Système d'Information de la Caisse Primaire Centrale d'Assurance Maladie des Bouches-du-Rhône (CPCAM131).



Avant de démarrer votre prestation, vous devez prendre connaissance de ces mesures élaborées à partir de la Politique de Sécurité du Système d'Information du Ministère Chargé des Affaires Sociales (PSSI MCAS) applicable à l'Assurance Maladie.

Accès aux sites

Tout accès aux sites de l'organisme doit être justifié par :

- Une demande d'intervention émanant des services concernés de l'Organisme,
- Une intervention programmée dans le marché,
- Le contenu de la prestation (ex. : gardiennage).

Les accès doivent s'effectuer aux jours ouvrés (du lundi au vendredi) et heures ouvrées (de 7h30 à 16h30), ou par dérogation, aux périodes autorisées par le marché.

Des moyens d'accès physiques permanents (ex. : clés, badges, codes d'accès) seront fournis contre émarquage aux prestataires assurant régulièrement des opérations de maintenance et d'entretien.

Les prestataires qui se rendent dans les locaux de l'Organisme doivent être désignés à l'avance par la société assurant la prestation.



Sans demande ou programmation préalable émanant des services de l'organisme, aucun intervenant ne sera autorisé à accéder aux sites de la CPCAM.

Accès aux locaux

Procédure d'accueil :

- Accéder aux locaux par l'entrée du public (prestataire sans moyen d'accès) ou du personnel (prestataire avec moyen d'accès),
- Se faire connaître dès l'arrivée auprès du Responsable d'Immeuble,
- Être systématiquement accompagné durant leur intervention, à l'aller comme au retour, d'un personnel habilité de l'Organisme.

Les intervenants ont l'obligation de :

- Porter en évidence le badge à l'effigie de leur société et mentionnant leurs noms et prénoms,
- Remplir la main courante lors de son arrivée et de son départ,
- Respecter les règles de sécurité en vigueur et présentées par voie d'affichage,
- Effectuer les travaux dangereux en application du plan de mesures inscrites dans le plan de prévention et présenter un permis de feu pour les travaux produisant des flammes ou de la chaleur,
- Compléter le bon d'intervention, le cahier de maintenance ou la main courante.



L'accès aux locaux techniques

Les locaux techniques (ex. : informatique, électrique) bénéficient d'un contrôle d'accès renforcé et nécessitent une habilitation spécifique. Les intervenants doivent être systématiquement accompagnés par un représentant de l'Organisme durant leur intervention dans ces locaux.

Confidentialité

Nous vous rappelons que votre société s'est engagée à respecter les clauses de confidentialité énoncées au contrat avec notre Organisme et à les faire respecter par son personnel et sous-traitant.

- Considérer comme strictement confidentiel, et s'interdire de divulguer, toute information, document, donnée ou concept dont il pourrait avoir connaissance.
- Toute information dont vous pouvez avoir connaissance est strictement réservée à un usage interne correspondant aux objectifs de la prestation.
- Prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse ainsi que toute divulgation à des tiers non autorisés.
- Ne prendre aucune copie de documents et supports d'informations qui vous sont confiés. Ils restent la propriété de la CPCAM des Bouches-du-Rhône.
- Prendre toutes les mesures de sécurité, notamment matérielles, pour assurer la conservation ainsi que l'intégrité des documents et informations traités.



Cette obligation s'applique en tout lieu (dans ou en dehors de l'organisme) et en tout temps (pendant et après le contrat de prestation selon la durée indiquée).

Prise en compte des principes de protection des données

Votre société et ses éventuels sous-traitants devront tenir compte des directives du Règlement Général sur la Protection des Données (RGPD).

- En cas de manipulation de traitement de données personnelles pour le compte de l'Organisme, vous devez respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation afin de répondre aux exigences du Règlement européen (RGPD), notamment n'accédez qu'aux documents et informations strictement nécessaires à la réalisation de la prestation.
- Les données auxquelles vous accédez sont strictement couvertes par le secret professionnel.



Conformément à l'article 122 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées au 6° de l'article 4 et à l'article 121.

Accès au Système d'Information

Conditions d'accès :

- Les accès au SI ne sont fournis aux prestataires que lorsque l'accès est absolument nécessaire à la réalisation de la prestation et qu'une demande a été effectuée par les services internes en charge du suivi de la prestation.
- En cas d'acceptation de la demande d'accès, un moyen d'authentification vous sera remis contre émargement.
 - Carte à puce et code associé pour un accès à partir d'un poste de travail.
 - Couple identifiant / mot de passe avec des droits spécifiques pour des accès sur des composants d'infrastructure.

Protection des moyens d'accès :

- Le code de la carte / le mot de passe ne doit ni être communiqué à une tierce personne ni être inscrit sur un support non protégé.
- Le mot de passe doit respecter certaines règles de constitution avec un nombre minimum de caractères.
- En cas de perte ou de vol, informer immédiatement votre référent de l'Organisme.



L'utilisation de matériels, logiciels et données informatiques mis à disposition dans le cadre de l'exécution de votre prestation nécessite le respect des procédures de gestion en vigueur et des règles de sécurité énoncées dans la Charte d'Utilisation des Ressources Informatiques.

Protection des composants du SI :

- Toute installation ou modification d'une infrastructure du SI (serveur, poste de travail, logiciel, réseau, téléphonie) ne peut être réalisée qu'après validation préalable et sous le contrôle du personnel informatique habilité de l'Organisme.

Protection des données :

- Le poste de travail ne peut être connecté sur un réseau non protégé,
- En cas d'absence à votre poste de travail, même de courte durée, verrouiller l'accès à la session,

- La configuration du poste de travail doit rester inchangée,
- N'utiliser un support amovible qu'après avoir contrôlé son contenu par l'antivirus,
- L'envoi de documents de l'organisme sur des mails personnels est interdit,
- Consulter uniquement les sites Internet nécessaires à votre activité.

Journalisation :

- Les accès et l'utilisation du Système d'information font l'objet d'une journalisation et sont périodiquement exploités par les agents habilités de l'Organisme.



Le prestataire devra mettre en place les mesures techniques et organisationnelles préconisées par l'Organisme de nature à empêcher tout accès ou utilisations frauduleuses des données et à prévenir toute perte, altération ou/et destruction des données.

Accès à distance au Système d'Information

Conditions d'accès :

- Les accès à distance au SI ne sont fournis aux prestataires que lorsque l'accès est absolument nécessaire à la réalisation de la prestation et qu'une demande a été effectuée par les services internes en charge du suivi de la prestation,
- Les engagements du prestataire concernant la télémaintenance, doivent être formalisés dans un document spécifique intitulé « Sécurité des télémaintenances », associé au marché.
- Le service informatique de l'Organisme mettra à disposition du prestataire les modalités techniques d'accès aux équipements télé-maintenus.

Déroulement :

- Les télémaintenances ne peuvent s'effectuer qu'au travers des outils de connexion suivants : TeamViewer ou WebEx.
- Le prestataire ne pourra utiliser aucune solution de prise en main à distance directe vers le poste utilisateur final.
- La session de télémaintenance ne doit pas pouvoir démarrer qu'après une demande formelle du prestataire et une autorisation explicite de l'Organisme.

- Le prestataire doit pouvoir fournir sur demande un rapport d'intervention mentionnant les dates et heures, la nature des interventions ainsi que le nom des intervenants.
- Durant toutes les actions de télémaintenance, il est nécessaire qu'un agent de l'Organisme soit présent.



- Le prestataire assurant la télémaintenance s'engage à n'accéder qu'aux seules ressources et informations strictement nécessaires à la télémaintenance.
- En particulier, il s'engage à ne pas rebondir sur d'autres machines de l'Organisme et à respecter la confidentialité des données potentiellement accédées.

Remontées d'incidents

Procédure de signalement :

- Les intervenants doivent signaler sans délai, tout incident de sécurité du SI détecté ou faille soupçonnée auprès du responsable d'Immeuble et/ou du suppléant, ou d'un personnel habilité.
- Toute initiative personnelle pour démontrer ou corriger la faille ou le dysfonctionnement détecté ou soupçonné est interdite.

Exemples d'incidents :

- Perte ou vol de moyens d'accès,
- Disparition ou vol de matériels ou de documents,
- Attaques virales,
- Contrôle d'accès neutralisé ou non opérationnel,
- Indisponibilité prolongée d'un dispositif de sécurité physique,
- ...



Le signalement d'un incident permet de renforcer la Sécurité du SI. Même en cas de doute, le prestataire ne doit pas hésiter à faire remonter son signalement.

Fin de prestation

Au terme de la prestation assurée pour l'Organisme (départ définitif, absence de longue durée ou/et à l'issue du marché), le prestataire doit restituer au représentant de l'Organisme l'intégralité des moyens d'accès physiques et logiques, la documentation, les données et supports informatiques qui ont pu être remis au cours de la prestation.

Procédure de sortie :

Le prestataire devra transmettre les matériels, documents et informations suivants à son correspondant de l'Organisme :

- 15 jours avant le départ

- Les savoirs et secrets utilisés dans le cadre de la prestation,
- Les informations sur les travaux en instance,

- Les mots de passe (généralistes).

- Le jour du départ

- Les clés accès locaux / badge accès aux locaux,
- Les moyens informatiques et téléphoniques mis à disposition,
- Les autres matériels logistiques,
- Les badges (carte agent, restaurant, parking...),
- Et les documents métier.



- Au moment du départ du prestataire, l'Organisme supprimera également l'ensemble des accès physiques et logiques utilisés par le prestataire.
- Le prestataire doit respecter les engagements de confidentialité et les obligations juridiques du contrat.

Sanctions applicables

En cas de non-respect par le prestataire d'une ou plusieurs règles de sécurité, l'organisme engagera une procédure auprès de la société afin que des sanctions soient appliquées au responsable.

Les sanctions seront adaptées aux manquements observés.

Par ailleurs, en cas de violation d'une disposition légale et réglementaire, la responsabilité civile et/ou pénale du prestataire, de ses préposés et/ou de ses sous-traitants pourra également être recherchée.



L'Organisme se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations et mesures de sécurité précitées par le prestataire.

Référents

Responsable d'immeuble :

..... Téléphone :
 Téléphone :
 Téléphone :

Sous-Direction Infrastructures et Services :

..... Téléphone :
 Téléphone :
 Téléphone :

Direction des Ressources :

..... Téléphone :
 Téléphone :

Contacts

MSSI : contact-ssi.cpam-marseille@assurance-maladie.fr

DPO : dpo.cpam-marseille@assurance-maladie.fr



Vous êtes maintenant prêt à réaliser votre prestation au sein de la CPCAM des Bouches-du-Rhône en respectant la sécurité du Système d'Information.

Nous comptons sur votre entière collaboration.

