

**MISSION DE MAITRISE D'ŒUVRE POUR LA RÉHABILITATION DE  
L'IMMEUBLE DU SIÈGE DE L'URSSAF DE LA CORSE**

**ANNEXE SECURITE INFORMATIQUE**

***Marché n° UR20-2026-003***

**DATE ET HEURE LIMITE DE RÉCEPTION DES OFFRES**

**Lundi 31 août 2026 – 12h00**

1. The first part of the paper discusses the importance of the study and the objectives of the research. It also provides a brief overview of the methodology used in the study.

2. The second part of the paper presents the results of the study. It includes a detailed analysis of the data and a discussion of the findings. The results show that there is a significant correlation between the variables studied.

3. The third part of the paper discusses the implications of the findings and provides recommendations for future research. It also includes a conclusion and a list of references.

## ANNEXE SECURITE INFORMATIQUE

### 1 Etat de l'art

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

#### 1.1 : Politique, organisation et gouvernance de la sécurité

**Politique de sécurité du titulaire :** le titulaire applique et fait appliquer à ses sous-traitants la politique de sécurité traitant notamment des thèmes suivants :

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

**Organisation de la sécurité adéquate :** le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.

**Existence d'un correspondant de sécurité :** le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation.

Ce correspondant est notamment l'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;

#### 1.2 Gestion des biens

**Séparation des données de l'acheteur et des données d'autres clients :** le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

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

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

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

**Maintien à jour et mise à disposition des données relatives à la prestation** : le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation.

Le titulaire fournit à la demande de l'acheteur toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

## 1.3 Sécurité Physique

**Changement de localisation géographique des services et des données** : en cas de changement de localisation des données ou services, le titulaire en informe préalablement l'acheteur.

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

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

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

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

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

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

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

**Protection intrusion physique des locaux techniques du titulaire :** les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements, informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j. Les moyens de protection sont adaptés aux moyens de détection et de réaction.

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

**Accompagnement des visiteurs :** le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

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

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

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

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

- La salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée ;
- Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multiclients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

## 1.4 Sécurité des réseaux et de l'exploitation

**Cloisonnement des environnements informatiques :** le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation. Il garantit notamment la confidentialité des données qui transitent par ses infrastructures ou celle de son sous-traitant. Il ne stocke ou ne fournit à un tiers aucune donnée transitant sur son réseau.

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

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

**Anti-virus opérationnel et à jour** : le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'acheteur.

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

**Sauvegarde des données** : le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par le chef de projet de l'acheteur dans le cadre de la prestation.

Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

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

**Comptes individuels** : le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation dispose d'un compte individuel qui peut être :

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

**Comptes obsolètes ou par défaut** ; le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

**Recensement des comptes d'accès** : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI contenant les données de l'acheteur ainsi que des rôles et privilèges qui y sont associés.

Il fournit cette liste à l'acheteur sur demande. Le titulaire effectue et formalise une revue périodique des comptes d'accès du titulaire aux ressources et données de l'acheteur utilisées dans le cadre de la prestation.

**Politique du moindre privilège** : le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

**Attaques en essai et erreurs sur secrets d'authentification** : les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

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

Le titulaire collecte et stocke à minima les informations suivantes :

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

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

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

**Politique de mot de passe** : sauf à ce que le titulaire ait généralisé l'authentification forte, il définit et fait respecter la politique de définition des mots de passe conforme à l'état de l'art et notamment aux recommandations de l'Anssi sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

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

## 1.5 Sécurité des postes de travail

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

**Chiffrement du poste de travail** : une solution de chiffrement, si possible qualifiée par l'Anssi, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles de l'acheteur stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

## 1.6 Traitement des incidents

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

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

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

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

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

## 1.7. Disponibilité des données et des systèmes d'information

Le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information durant toute la durée du marché conformément aux exigences formulées par le chef de projet de l'acheteur dans le cadre de la prestation.

## 1.8 Continuité des activités

**Plan de continuité d'activité** : le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat. Il fournit, à la demande de l'acheteur, la preuve de l'existence d'un plan de continuité d'activité régulièrement testé pour l'ensemble des services fournis à l'acheteur.

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

**Incident affectant la continuité des services** : En cas d'incident affectant la continuité des services, le titulaire contacte le Centre Opérationnel de l'ACOSS à l'adresse [cos@acoss.fr](mailto:cos@acoss.fr).

## 1.9. Conformité, audit, inspection, contrôle

**Autocontrôles de sécurité** : le titulaire effectue des autocontrôles de conformité aux exigences de la présente annexe pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

**Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur** : en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de

remédiation devra être formalisé par le titulaire 15 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

## 2. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire

**Respect des exigences de sécurité de l'acheteur :** au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (charte utilisateur, etc.).

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

**Interconnexion des SI de l'acheteur et du titulaire :** en cas d'interconnexion des SI de l'acheteur et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'acheteur.



# Annexes

## 1. Les principaux documents applicables

### Les documents internes de l'acheteur

Exemples : la PSSI de l'acheteur, le dossier d'homologation d'un système d'information

### Les documents externes

Les documents suivants (*liste non exhaustive*) accessibles à partir du site de l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI), dans leur version à leur date de publication, peuvent servir de référence dans la rédaction des contrats de l'acheteur :

#### Réglementation

- L'instruction interministérielle N°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)  
<http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/>
- L'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale <http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/>
- La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)  
<http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/>
- Le référentiel général de sécurité (RGS V2)  
<http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/>

#### Guides

- Le guide « Maîtriser les risques de l'infogérance »  
[http://www.ssi.gouv.fr/IMG/pdf/2010-12-03\\_Guide\\_externalisation.pdf](http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf)
- Les recommandations et bonnes pratiques associées aux sujets ci-dessous :  
<http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/>
  - [Authentification et mécanismes cryptographiques](#) ;
  - [Sécurité du poste de travail et des serveurs](#) ;
  - [Sécurité de la messagerie](#) ;

- Sécurité des médias amovibles ;
- Sécurité des liaisons sans fil ;
- Sécurité des copieurs ou imprimantes multifonctions ;
- Sécurité des solutions de mobilité ;
- Sécurité des réseaux ;
- Sécurité des applications WEB ;
- Sécurité de l'externalisation ;
- Réaction en cas d'incident ;
- Sécurité des systèmes industriels.

*(Liste non exhaustive)*

- Les guides de bonnes pratiques de la CNIL pour la protection des données à caractère personnel [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/Guide\\_securite-VD.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf)
- Le guide **« Achats informatiques et propriété intellectuelle »** élaboré de manière conjointe par l'APIE, la Direction interministérielle des systèmes d'information et de communication de l'État (DINSIC) et la Direction des achats de l'État (DAE)

2. Modèle de formulaire d'engagement et de déclaration de connaissance des règles de discrétion, de confidentialité et de sécurité informatique

**ENGAGEMENT DE RECONNAISSANCE DE RESPONSABILITE**

Relatif au respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur à [entité]

L'URSSAF de la Corse

**LA PERSONNE DESIGNEE CI-APRES :**

|                                                                                                 |  |     |  |
|-------------------------------------------------------------------------------------------------|--|-----|--|
| NOM – Prénom :                                                                                  |  |     |  |
| Né(e) le :                                                                                      |  | à : |  |
| déclarant avoir toute autorité pour agir en tant que<br><i>(fonctions dans l'entreprise) :</i>  |  |     |  |
| au nom de la société désignée ci-contre<br><i>(raison sociale et adresse du siège social) :</i> |  |     |  |

dans le cadre de l'exécution du marché public xxx, UR20-2026-003



**Reconnaît avoir été sensibilisée et de ce fait avoir pleinement connaissance :**

- que l'autorisation d'accès aux locaux de l'acheteur est conditionnée à l'obtention d'une autorisation d'accès délivrée après enquête diligentée par le service de sécurité compétent, ce droit d'accès est strictement personnel, incessible et limité dans le temps ;
- que toute éventuelle action contraire aux règles édictées doit être immédiatement signalée à la [mettre le nom de la direction] et à sa voie fonctionnelle SSI ;
- que l'acheteur peut, à tout instant, demander à en contrôler sans restriction l'utilisation qui en est faite ;
- des dispositions générales relatives à la réglementation et à la législation française en vigueur dans le domaine de la sécurité des systèmes d'information et plus particulièrement à la fraude informatique, notamment les articles 323-1 à 323-3-1 du code pénal ;
- des dispositions de l'instruction interministérielle n°901 sur la protection des systèmes d'information sensibles ;
- des dispositions des articles 413-9 à 413-12 du code pénal relatifs aux atteintes au secret de la défense nationale ;
- des dispositions de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale ;
- qu'un dispositif (journalisation des notifications techniques et de sécurité) permet d'assurer la traçabilité de l'ensemble des actions menées sur le système d'information, pour raisons de sécurité.

**M'engage à ce que tous les agents appelés, sous ma responsabilité, à intervenir à un titre quelconque dans le cadre de l'exécution du marché :**

- respectent l'obligation de discrétion professionnelle pour tous les faits, informations ou documents dont ils auraient connaissance dans l'exercice ou à l'occasion de l'exercice de leurs activités ;
- ne divulguent en aucun cas à un tiers des informations ou données tant personnelles que professionnelles qu'ils pourraient être amenés à apprendre dans l'exercice de leur mission ;
- ne reproduisent, ni ne stockent, ni ne copient, ni ne diffusent, ni ne modifient, ni n'altèrent, ni ne détruisent toute information ou donnée dont ils pourraient avoir connaissance à d'autres fins que celles de l'exercice de leur mission ;
- respectent le principe fondamental du « besoin d'en connaître » et ainsi ne tentent pas d'accéder, ni de reproduire, ni de stocker, ni de copier, ni de diffuser, ni de modifier, ni d'altérer, ni de détruire toute information dont ils ne sont pas supposés avoir connaissance dans l'exercice de leur mission.

**M'engage à ce que tous les agents disposant d'un accès à un système d'information de l'administration et, par conséquent, d'un compte nominatif :**

- ne tentent pas de connecter tout appareil électronique communicant ou non, personnel ou de la société, au système d'information sans avoir reçu préalablement l'autorisation formelle de la voie fonctionnelle SSI ;
- ne modifient pas sans autorisation la configuration des moyens mis à leur disposition et notamment ne raccordent pas de moyens informatiques qui n'auront pas été convenus au préalable avec l'acheteur dans le cadre de la définition de l'architecture ;
- ne se livrent pas à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels ils ont accès ;

- ne mettent pas à la disposition d'utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services ;
- ne perturbent ni n'interrompent le fonctionnement normal du système d'information ou de l'un de ses composants ;
- n'installent pas, sans autorisation préalable et formelle de la voie fonctionnelle SSI (ou de son représentant) de logiciels sur le système d'information ou sur les équipements mis à leur disposition ;
- n'introduisent, ni ne testent, ni n'utilisent des supports informatiques ou médias dont l'origine leur est inconnue, douteuse ou incertaine ;
- ne génèrent pas volontairement ou involontairement des perturbations sur les ressources du SI que ce soit par des manipulations anormales ou par l'introduction illicite de logiciels contrefaits ou piratés potentiellement nuisibles en termes de failles de sécurité ou de pollution virale.

**Déclare être pleinement consciente de mes responsabilités et reconnaît être informée des conséquences pénales et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci-dessus.**

|                                                                             |  |                        |  |
|-----------------------------------------------------------------------------|--|------------------------|--|
| A                                                                           |  | le                     |  |
| Recopier ci-dessous la formule manuscrite suivante : « <i>je m'engage</i> » |  |                        |  |
|                                                                             |  |                        |  |
| CACHET DU TITULAIRE                                                         |  | SIGNATURE DU TITULAIRE |  |
|                                                                             |  |                        |  |

