ENGAGEMENT DE RECONNAISSANCE DE RESPONSABILITE

relatif au bon respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur au ministère de l'intérieur

LA PERSONNE DÉSIGNÉE CI-APRÈS **:**

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

dans le cadre de l'exécution du Présent marché.

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

- que l'autorisation d'accès aux locaux de l'administration 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 DNUM et à sa voie fonctionnelle SSI ;
- que l'administration 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 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.

S'engage à ce que tous les agents appelés, sous sa 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 ;
- prennent connaissance et respectent les dispositions décrites en annexe I du ccp relative à la protection des informations, à la confidentialité et aux mesures de sécurité ;
- 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.

S'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 de télécommunication et informatiques qui n'auront pas été convenus au préalable avec le ministère de l'Intérieur 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 ses responsabilités et reconnait 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 : « ***je m'engage*** »			
CACHET DE L'ENTREPRISE		**SIGNATURE**	