PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général du Gouvernement

Direction des services
administratifs et financiers

Annexe 5 au cahier des clauses techniques et particulières

-

Règles de sécurité applicables au titulaire

ARTICLE 5 – HOMOLOGATION DE SECURITE

La circulaire n°5725 en date du 17 juillet 2014 et l'arrêté du Premier ministre en date du 6 mai 2010 portant respectivement sur la Politique de sécurité des systèmes d'information de l'état et approbation du Référentiel général de sécurité imposent ou recommandent aux Autorités Administratives un ensemble de dispositions. Celles-ci conduisent à la mise en œuvre de mesures de sécurité qui adressent toutes les dimensions d'un système d'information : humaine, organisationnelle ou technologique.

In fine, tous ces systèmes font l'objet d'une démarche d'homologation dans un cadre défini par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Son objectif est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire. L'homologation de sécurité permet à un responsable, en s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré.

Le présent système de contrôle d'accès et de vidéo surveillance entre dans ce contexte et son étude d'homologation a été initiée sur la base du référentiel général de sécurité (lien : RGS) ainsi que sur le dossier relatif à la politique de sécurité des systèmes d'information de l'État (PSSIE) dont la DILA a produit une déclinaison.

En annexe I du présent document est joint l'ensemble des mesures PSSIE dans leur déclinaison DILA qui s'attachent au système actuel de contrôle d'accès et de vidéo-surveillance et qui feront l'objet d'un examen lors du processus d'homologation.

Hormis ces dispositions, il est précisé que l'ensemble des moyens informatiques servant le présent système d'information devra rester isolé du reste des moyens informatiques DILA, ainsi qu'il l'est actuellement.

ANNEXE 1 – LISTE DES DISPOSITIONS PSSIE APPLICABLES

Chacune des dispositions de la PSSIE a été formalisée ici de manière à s'adapter au fonctionnement attendu des prestations fournies à la DILA. **Il convient donc d'en faire une lecture transposée au système d'information objet de ce marché**. L'ensemble des réponses à ces mesures différentes clauses peut être présenté dans un document formalisé type Plan d'Assurance Sécurité (PAS) ou tout autre document du même type.

Section	Titre	Clause SSI
1. État de l'art	Conformité à l'état de l'art	Le titulaire conçoit, met en œuvre et exploite les systèmes d'information sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information.
1. État de l'art	Référence aux guides ANSSI	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. État de l'art	Exigences pour les interfaces web	Les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ; les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ; l'utilisation de la technologie HSTS est fortement recommandée ; les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ; une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité : X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ; les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
1. État de l'art	Exigences pour les services de courriels	Les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ; la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC)).

2.1. Spécifications techniques et utilisation de labels	Utilisation de spécifications techniques ou de labels	L'acheteur définit ses besoins et les prestations à réaliser par référence à des spécifications techniques ou par l'utilisation de labels. Un label est tout document, certificat ou attestation qui prouve que les produits, les services, les procédés ou les procédures en rapport avec l'objet du marché remplissent certaines caractéristiques. Lorsqu'un acheteur exige un label particulier, celui-ci est tenu d'accepter les labels équivalents qui confirment que les caractéristiques exigées sont remplies.
2.1. Politique, organisation, gouvernance	Politique de sécurité du titulaire	Le titulaire applique et fait appliquer à ses sous-traitants une politique de sécurité couvrant notamment : - 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.
2.1. Politique, organisation, gouvernance	Correspondant 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. Ce correspondant est joignable aux horaires suivants (à compléter). Tout remplacement de ce correspondant doit être notifié à l'acheteur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.
2.1. Politique, organisation, gouvernance	Gestion des risques	Le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.
2.1. Politique, organisation, gouvernance	Gestion de crise sécurité	Le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés. Ce plan précise au minimum : les principes d'escalade (critères de déclenchement, synoptique d'escalade), la composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire).
2.2. Gestion des biens	Séparation des données	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

2.2. Gestion des biens	Protection de la documentation papier	Protection de la documentation de l'acheteur sur support papier : le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.
2.2. Gestion des biens	Modalités d'échanges d'informations	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.
2.2. Gestion des biens	Échange de supports	Échange 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.
2.2. Gestion des biens	Transmission de fichiers sur support physique	Transmission de fichiers sur un support physique : toute transmission de fichiers sur un support physique (DAT, CDROM, etc.), par courrier externe ou par porteur, donne lieu à un accusé de réception. Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'acheteur. De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant : -l'émetteur et le destinataire ; - le détail des opérations de transferts et notamment le nombre, la date. Sur simple demande, ce registre est mis à la disposition de l'acheteur adjudicateur par le titulaire.
2.2. Gestion des biens	Marquage des ressources techniques	Marquage des ressources techniques : le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.
2.2. Gestion des biens	Supports de stockage en fin de vie	Supports de stockage hébergeant des données de l'acheteur : 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. Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.
2.2. Gestion des biens	Mise à disposition des données	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 systématiquement toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

2.3 Sécurité physique	Changement de localisation	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.
2.3 Sécurité physique	Hébergement de données	Hébergement de données : à 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.
2.3 Sécurité physique	Contrôle d'accès physique aux bâtiments	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.
2.3 Sécurité physique	Protection des locaux techniques	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
2.3 Sécurité physique	Protection intrusion physique des locaux techniques du titulaire	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.

2.3 Sécurité physique	Accompagnement des visiteurs	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.
2.3 Sécurité physique	Protection des plateaux mutualisés	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.).
2.3 Sécurité physique	Étanchéité physique des ressources informatiques	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 multi-clients, 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.
2.4. 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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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.

2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	Comptes individuels	Le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'acheteur) 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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	Comptes techniques	Dans le cadre de la cartographie du système d'information prévue, le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, etc.) nécessaires au fonctionnement du système.
2.4. Sécurité des réseaux et de l'exploitation	Recensement des comptes d'accès	Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants 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 aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	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 a 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.
2.4. Sécurité des réseaux et de l'exploitation	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.
2.4. Sécurité des réseaux et de l'exploitation	Politique de mot de passe	Le titulaire respecte la politique de définition des mots de passe de l'acheteur sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.
2.5. Sécurité du poste de travail	Protection contre le vol 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.
2.5. Sécurité du poste de travail	Chiffrement du poste de travail	Chiffrement du poste de travail : une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles

2.6. Traitement des incidents	Enregistrement et traçabilité des incidents	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.
2.6. Traitement des incidents	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).
2.7. Disponibilité des données et des systèmes d'information	Disponibilité des données et des systèmes	Durant le marché, le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information dans un délai maximum d'un jour ouvré.
2.8. Continuité des services	Plan de continuité d'activité	Le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat dans les délais maximum suivants : un jour ouvré. 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.
2.8. Continuité des services	Remplacement du matériel endommagé ou perdu	Le titulaire prend toutes les dispositions nécessaires (matériel en spare, contrats de service), en relation avec l'acheteur, pour remplacer rapidement et sur les différents sites de l'acheteur tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).
2.9. Conformité, audit, inspection, contrôle	Autocontrôles de sécurité	Le titulaire effectue des autocontrôles de conformité aux exigences du CCTP/PAS pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.
2.9. Conformité, audit, inspection, contrôle	Régularisation des écarts ou des non-conformités	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.
3. Obligations pour les titulaires intervenant au	Respect des exigences de	Au même titre que les agents de l'acheteur, le titulaire doit prendre connaissance et appliquer les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

sein des locaux de l'acheteur	sécurité de l'acheteur	
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Respect des standards et méthodologies de l'acheteur	Le titulaire doit respecter les standards et les méthodologies préconisées au sein de l'acheteur.
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Respect du périmètre de la prestation	Le titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Connexion d'équipements au réseau de l'acheteur	Le titulaire doit connecter sur le réseau interne de l'acheteur uniquement des équipements fournis par l'acheteur. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.).
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Inventaire des composants mis à disposition par l'acheteur	Le titulaire met en place une solution pour élaborer et maintenir un inventaire complet et à jour des composants mis à disposition par l'acheteur. Cette liste devra être transmise régulièrement à l'acheteur.
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Recensement des comptes d'accès	Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés. Il doit être en mesure de fournir cette liste à l'acheteur sur demande. Le titulaire doit également effectuer et formaliser une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Restitution des équipements fournis par l'acheteur	À la fin de la prestation, le titulaire doit restituer l'ensemble du matériel fourni par l'acheteur.
3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur	Restitution des informations collectées par le titulaire	À la fin de la prestation, le titulaire doit restituer ou détruire les informations de l'acheteur en sa possession. Un procès-verbal de destruction des données doit être signé par le titulaire.
4. Obligations pour les titulaires intervenant en situation d'astreinte	Astreinte	Le titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements. Les cas de force majeure doivent également être couverts.
4. Obligations pour les titulaires intervenant en situation d'astreinte	Sécurisation des flux d'astreinte	Le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN, IPSec) pour la connexion à distance en astreinte aux réseaux utilisés dans le cadre de la prestation (que ce soient ceux du titulaire, ceux de l'acheteur ou les deux éventuellement).
4. Obligations pour les titulaires intervenant en situation d'astreinte	Chiffrement des postes d'astreinte	Le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte.
4. Obligations pour les titulaires intervenant en	Authentification forte	Le titulaire rend obligatoire l'utilisation de l'authentification forte (ex. badge, token) au poste de travail utilisé en astreinte.

situation d'astreinte		
4. Obligations pour les titulaires intervenant en situation d'astreinte	Connexion distante	Le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires ouvrés), et aux ressources nécessaires en astreinte uniquement.
4. Obligations pour les titulaires intervenant en situation d'astreinte	Enregistrement des accès	Dans le cas où l'acheteur autorise la Prise en Main À Distance (PMAD) de ses infrastructures, le titulaire enregistre et sécurise les accès distants au SI de l'acheteur.
4. Obligations pour les titulaires intervenant en situation d'astreinte	Suivi des interventions	Le titulaire est capable de fournir à l'acheteur, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'acheteur en astreinte.
5. 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 (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).
5. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire	Respect des standards et méthodologies de l'acheteur	Le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur.

5. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire	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.
5. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire	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. Pour chaque interconnexion, les éléments suivants doivent être définis : · les flux et protocoles autorisés ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ; · les modalités d'authentification requises : authentification par mot de passe, authentification forte par mot de passe unique ou par certificat ; · les modalités e chiffrement des échanges : le chiffrement de flux transitant sur Internet est requis ; · les exigences spécifiques de traçabilité des accès ; ·les moyens de sécurité complémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif…
6.1. Prestations d'études	Respect des standards et méthodologies de l'acheteur	Le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'acheteur. En particulier, le titulaire doit appliquer les méthodes d'évaluation de la sensibilité et d'analyse de risques des systèmes d'information lorsqu'il intervient dans les phases amont des projets.
6.1. Prestations d'études	Ségrégation des environnements	Le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
6.1. Prestations d'études	Conduite des tests	Lors de la conduite de tests de validation ou du déploiement, le titulaire doit utiliser des données de tests anonymisées (sauf accord explicite de l'acheteur) ; ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de test ; remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible.

6.2. Prestations de développement	Utilisation du cadre standard de développement	Le titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) de l'acheteur comprenant notamment l'organisation des équipes de développement et de la prestation, les configurations matérielles préconisées pour le développement, les outils de développement préconisés par l'acheteur (logiciels, versions, etc.), une structure de développement (framework) intégrant les fonctions de sécurité.
6.2. Prestations de développement	Propriété du code	L'acheteur est propriétaire du code et des droits de propriété intellectuelle des éléments développés dans le cadre de la prestation.
6.2. Prestations de développement	Ségrégation des environnements	Le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
6.2. Prestations de développement	Protection des codes sources	Le titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.
6.2. Prestations de développement	Documentation du code	Le titulaire doit commenter et documenter le code développé dans le cadre de la prestation. La documentation doit être mise à jour régulièrement.
6.2. Prestations de développement	Traçabilité des actions de développement	Toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure.
6.2. Prestations de développement	Sauvegarde des codes sources	Le titulaire doit sauvegarder et conserver chaque version du code source recettée dans le cadre de la prestation. Les accès à ces sauvegardes devront être tracés.
6.2. Prestations de développement	Dépôt des codes source	Le titulaire doit déposer les codes sources dans ses différentes versions et mises à jour selon les recommandations de l'acheteur.
6.2. Prestations de développement	Conduite des tests	Lors de la conduite de tests de validation ou du déploiement, le titulaire doit utiliser des données de tests anonymisées ; ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de

		test ; remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible ; ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente.
6.2. Prestations de développement	Contrôle de la qualité et de la sécurité du développement	L'acheteur se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le titulaire, via des audits et/ou des tests d'intrusion par exemple (audit de code sur les parties les plus sensibles, etc.).
6. Prestations d'hébergement	Respect de la directive de sécurité de l'hébergement informatique de l'acheteur	Le titulaire doit respecter les exigences de la directive de sécurité de l'hébergement informatique de l'acheteur.
6.4. Prestations d'achat de matériels/logiciels	Absence de failles à la mise en production	Le titulaire s'engage à ce que les produits du contrat soient, au jour de leur mise en production pour l'acheteur, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations.
6.4. Prestations d'achat de matériels/logiciels	Détection d'une vulnérabilité	En cas de mise en évidence d'une vulnérabilité affectant un produit du contrat, le titulaire doit mettre à disposition de l'acheteur dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du produit concerné. Le titulaire collabore également avec l'acheteur pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.
6.4. Prestations d'achat de matériels/logiciels	Exigences liées à la maintenance	Dans le cadre d'une opération de maintenance, le titulaire s'engage à chiffrer ou effacer de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique de l'acheteur. Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe locale chargée des systèmes d'information. Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est interdit.

6.4. Prestations d'achat de matériels/logiciels	Exigences liées à la télémaintenance	Dans le cadre d'un accès de télémaintenance à une ressource informatique (matériel, logiciel) de l'acheteur, le titulaire doit présenter des mesures de sécurité renforcées validées par l'acheteur. Exemples de mesures de sécurité renforcées : sécurisation de l'infrastructure de raccordement réseau, mise en place de mots de passe spécifiques pour l'accès en télémaintenance, respectant des règles de robustesse et de renouvellement, activation sur demande des accès entrant en télémaintenance, journalisation des accès en télémaintenance, interdiction des possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local de l'acheteur et plus largement vers les réseaux inter-urbains (WAN) nationaux.
6.4. Prestations d'achat de matériels/logiciels	Exigences liées à la qualification	En cas d'achat de produits de sécurité qualifiés, il est nécessaire de se référer au guide d'achat des produits qualifiés de l'ANSSI. Si le produit vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement. Exemples de mesures de sécurité renforcées : · Sécurisation de l'infrastructure de raccordement réseau (cf. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire) ; · Mise en place de mots de passe spécifiques pour l'accès en télémaintenance, respectant des règles de robustesse et de renouvellement ; · Activation sur demande des accès entrant en télémaintenance. Par défaut, les accès entrants doivent être inactifs ; · Journalisation des accès en télémaintenance ; · Interdiction des possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local de l'acheteur et plus largement vers les réseaux inter-urbains (WAN) nationaux.
6.4. Prestations d'achat de matériels/logiciels	Mise au rebut	Pour tout départ définitif d'un matériel ou logiciel du service, le titulaire doit empêcher de manière sécurisée l'accès aux données présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l'acheteur. En cas d'impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le disque dur ou la mémoire doit être détruit(e) physiquement avant de quitter définitivement le service ou démonté(e) et entreposé(e) sur site dans un local sécurisé en attente de destruction.