

**ANNEXE 6 AU CCAP  
CLAUSES ADMINISTRATIVES PARTICULIERES SPECIFIQUES AU LOT N°6**

## TABLE DES MATIERES

Article 1 -	CONTEXTE.....	3
Article 2 -	LIEUX D'EXECUTION.....	3
Article 3 -	INFORMATION SUR LES VULNERABILITES ET INCIDENTS DE SECURITE DETECTES SUR LE SYSTEME D'INFORMATION DU TITULAIRE.....	3
Article 4 -	PENALITES POUR VIOLATION DES OBLIGATIONS DE SECURITE OU DE CONFIDENTIALITE .....	3
Article 5 -	AUDIT DE SECURITE.....	4
Article 6 -	MISE A JOUR ET NOUVELLES VERSIONS DE LOGICIELS - DOCUMENTATION.....	4
Article 7 -	MAINTIEN EN CONDITION DE SECURITE .....	5
Article 8 -	VERIFICATIONS QUALITATIVES .....	5
Article 9 -	GARANTIE .....	6
Article 10 -	MAINTENANCE, TIERCE MAINTENANCE APPLICATIVE .....	6
Article 11 -	STIPULATIONS COMMUNES .....	7

## Article 1 - CONTEXTE

Le cahier des clauses administratives particulières (CCAP) s'applique à tous les lots de l'accord-cadre y compris le lot n°6 - Système d'information et bornes de gestion. Toutefois, le présent document précise les clauses administratives propres au lot n°6. En cas de contradiction entre les clauses générales du CCAP et les clauses spécifiques du présent document, ces dernières prévalent sur les clauses du CCAP.

Au sens du présent document :

- le « logiciel » est une œuvre constituée d'un ensemble de programmes, procédés et règles, relatifs au fonctionnement d'un ensemble de traitement de données et la documentation afférente. Le terme logiciel employé seul dans le présent document désigne indifféremment des logiciels standards ou des logiciels spécifiques ;
- le « logiciel standard » est un logiciel conçu par le titulaire ou un éditeur tiers, pour être fourni à plusieurs utilisateurs en vue de l'exécution d'une même fonction ;
- le « logiciel spécifique » est un logiciel spécialement développé par le titulaire pour apporter une solution sur mesure aux besoins propres de l'acheteur. Il peut s'agir d'une œuvre originale créée ex nihilo, ou de l'adaptation, au moyen de développements spécifiques, d'œuvres préexistantes (logiciels standards ou logiciels spécifiques) ;
- l'application est un ensemble de logiciels nécessaires pour l'exécution d'une tâche donnée.

S'ajoute pour le lot n° 6 les pièces contractuelles suivantes le cas échéant :

- l'offre technique du titulaire et ses éventuelles annexes dont, le cas échéant, le plan d'assurance sécurité (PAS), le plan d'assurance qualité et/ou le plan de prévention des risques (PPR) ;
- le cas échéant, le plan de sécurité des systèmes d'information (PSSI).

Ces deux pièces s'ajoutent en bas de la liste de l'article 8 du CCAP, et ont donc une valeur inférieure aux autres pièces citées.

Le titulaire doit être propriétaire du logiciel de gestion et des plans de fabrication de la borne de façon à être en mesure d'apporter des modifications au logiciel et à la borne en garantissant le respect des exigences de sécurité du Ministère des Armées et des Anciens Combattants.

## Article 2 - LIEUX D'EXECUTION

L'acheteur définira en début d'exécution du présent marché les règles d'accès aux sites concernés.

## Article 3 - INFORMATION SUR LES VULNERABILITES ET INCIDENTS DE SECURITE DETECTES SUR LE SYSTEME D'INFORMATION DU TITULAIRE

Pour les prestations objet du lot n°6, le titulaire met à disposition un dispositif d'information dédié à la sécurité informatique (notamment flux RSS/ATOM, liste de diffusion par courriel ou autre). Ce dispositif vise à tenir l'acheteur informés des événements et changements impactant la sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel si le traitement des données est sous-traité au titulaire), et des mesures correctives ou conservatoires à appliquer.

## Article 4 - PENALITES POUR VIOLATION DES OBLIGATIONS DE SECURITE OU DE CONFIDENTIALITE

En cas de violation des mesures de sécurité ou de l'obligation de confidentialité énoncées à l'article 9.4.4 du CCAP, le titulaire s'expose aux pénalités suivantes, appliquées dans les conditions prévues 9.12 du CCAP :

- en cas de non-respect des règles de sécurité et de protection des informations confidentielles n'impliquant pas des données à caractère personnel : application d'une pénalité égale à 0,5 % du montant exécuté du bon de commande, à la date de constatation du fait générateur ;

- en cas de non-respect des règles de sécurité et de protection des informations confidentielles impliquant des données à caractère personnel : application d'une pénalité égale à 2 % du montant exécuté du bon de commande, à la date de constatation du fait générateur.

Toutefois, l'application de ces pénalités n'entraîne pas renonciation par l'acheteur d'engager, le cas échéant, la responsabilité extracontractuelle et pénale du titulaire.

#### Article 5 - AUDIT DE SECURITE

L'acheteur peut effectuer ou faire effectuer un audit de sécurité auprès du titulaire, ou le cas échéant de ses sous-traitants, afin de s'assurer de la prise en compte effective du niveau de sécurité requis par l'acheteur.

Le titulaire est informé quinze jours à l'avance (date de l'audit, modalités financières pour l'acheteur et le titulaire, etc.).

L'acheteur, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter du terme de l'exécution de l'accord-cadre ou de sa résiliation, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

#### Article 6 - MISE A JOUR ET NOUVELLES VERSIONS DE LOGICIELS - DOCUMENTATION

##### 6.1. Mises à jour et nouvelles versions de logiciels :

Lorsque les prestations comprennent la livraison de logiciels standards ou de logiciels spécifiques, elles comprennent également, pendant la durée du marché, la livraison des mises à jour qui leur sont apportées ainsi que la livraison des nouvelles versions.

Le prix de ces mises à jour ou de ces nouvelles versions est inclus dans le prix du marché.

##### 6.2. Documentation technique :

Le titulaire livre, avec chaque matériel ou chaque logiciel, une documentation technique en langue française indiquant les modalités de leur mise en fonction. Il en est de même à chaque livraison de mise à jour ou de nouvelle version de logiciel.

La documentation est un ensemble d'informations relatives au logiciel, qui peut être, en tout ou partie, une connaissance antérieure qu'il s'agisse d'un logiciel diffusé sous une licence éditeur propriétaire ou publié sous le régime de la licence libre, et qui contient tout ou partie des éléments suivants :

- le descriptif détaillé des environnements techniques matériels et logiciels de développement, d'intégration et, le cas échéant, de fonctionnement ainsi que les documentations techniques de développement et de maintenance correspondantes ;
- les procédures de fabrication/intégration du résultat depuis l'installation de l'environnement de développement et d'intégration, la lecture, le chargement, les opérations de compression/décompression des supports fournis ainsi que la compilation des sources déposées, l'intégration, jusqu'à la production d'une version livrable ;
- la documentation de conception et les documentations techniques associées telles que les dossiers techniques de conception, les dossiers d'études techniques, les dossiers de spécifications, les schémas de base de données, modèles conceptuels et physiques de données concernant les données échangées entre les bornes et le SI central, ainsi que les données qui seront importées et exportées des bornes ou bien du SI central ;
- les dossiers d'études techniques, de paramétrage, d'installation, de configuration, d'exploitation et de maintenance ;
- les standards de programmation et de documentation, les dossiers et plans de test ;
- la documentation préalable à la conception des logiciels telle que notamment le cahier des charges et le document de présentation des besoins standards liés à l'utilisation des logiciels ;
- la documentation d'utilisation (manuel de l'utilisateur, aide en ligne) ;
- la documentation d'installation, d'exploitation, de maintenance et de manière générale tout élément permettant à la personne publique d'utiliser, d'exploiter le résultat ainsi que de maintenir le résultat, seul ou par le biais d'un tiers prestataire.

Le prix de cette documentation technique est inclus dans le prix du marché.

La documentation doit être transmise au plus tard à la livraison du matériel, du logiciel, de chaque mise à jour ou nouvelle version le cas échéant.

## Article 7 - MAINTIEN EN CONDITION DE SECURITE

Traitement des obsolescences :

Le titulaire n'utilise que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée de l'accord-cadre. Si la durée de l'accord-cadre dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus présentant des caractéristiques équivalentes et qui répondent en tous points aux exigences du marché.

Le titulaire élabore, tient à jour et met en œuvre une procédure de maintien en condition de sécurité de toutes les ressources dont il a la charge. Cette procédure prévoit :

- les délais d'application des mises à jour de sécurité en fonction du niveau de risque associé ;
- une définition des cas d'urgence précisant explicitement les motifs de déclenchement et les exceptions au cas nominal qui sont induites ;
- la marche à suivre dans le cas où l'application d'une mise à jour de sécurité échoue.

Le titulaire tient à jour l'inventaire de l'ensemble des logiciels et micrologiciels mettant en œuvre le service. Cet inventaire doit identifier pour chaque logiciel, sa version et les équipements sur lesquels le logiciel est installé.

A cette fin, le titulaire élabore, tient à jour et met en œuvre une procédure de maintien en condition de sécurité de toutes les ressources dont il a la charge. Cette procédure prévoit :

- les délais d'application des mises à jour de sécurité en fonction du niveau de risque associé ;
- une définition des cas d'urgence précisant explicitement les motifs de déclenchement et les exceptions au cas nominal qui sont induites ;
- la marche à suivre dans le cas où l'application d'une mise à jour de sécurité échoue.

Le titulaire installe et maintient les dispositifs du service dans des versions stables et à jour de leurs correctifs de sécurité et conformément à la procédure de maintien en condition de sécurité. Les versions installées doivent être des versions supportées sauf si celles-ci empêchent la réalisation du service. Il vérifie l'impact de l'installation des mises à jour sur le système d'information du service. Dans le cas où l'impact de l'installation ne permet pas la réalisation du service, le titulaire en documente les raisons, et définit et met en œuvre des mesures de réduction des risques.

Le titulaire devra s'assurer de l'authenticité et de l'intégrité des mises à jour téléchargées auprès des sources de mise à jour de confiance.

Correctifs de sécurité :

Une vérification d'aptitude (VA) ou une vérification de service régulier (VSR) peut être refusée si des composants ne sont pas à jour des correctifs de failles de sécurité publiés par l'éditeur depuis un délai supérieur à trois mois. L'acheteur définit les fréquences des livraisons en coordination avec les équipes d'exploitation, en fonction des différentes criticités des vulnérabilités concernées.

Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l'application du correctif.

## Article 8 - VERIFICATIONS QUALITATIVES

8.1. Les opérations de vérification qualitatives ont pour objet de permettre à l'acheteur de contrôler notamment que le titulaire :

- a mis en œuvre les moyens définis dans le marché, conformément aux prescriptions qui y sont fixées ;
- a réalisé les prestations définies dans le marché comme étant à sa charge, conformément aux

dispositions contractuelles.

Les opérations de vérifications qualitatives ont également pour objet de contrôler les conformités à la politique de sécurité. L'acheteur apprécie l'enjeu de la non-conformité à la politique de sécurité eu égard à la sensibilité des données manipulées, leurs volumes et les conséquences prévisibles si la non-conformité persiste. En fonction de cette analyse, ces non conformités peuvent avoir pour conséquence l'ajournement, le rejet ou l'admission des prestations avec réfaction.

Pour les matériels et les logiciels, l'acheteur vérifie que les prestations sont conformes aux stipulations du marché et aux bancs d'essais lorsque l'acheteur a choisi d'y recourir.

8.2. Les opérations de vérifications qualitatives comprennent deux étapes : la vérification d'aptitude et la vérification de service régulier.

8.3. La vérification d'aptitude intervient après la mise en ordre de marche. Elle a pour objet de constater que les prestations, livrées ou exécutées, présentent les caractéristiques techniques qui les rendent aptes à remplir les fonctions précisées dans les documents particuliers du marché.

Cette constatation peut aussi résulter de l'exécution, dans les conditions fixées par le marché, d'un ou de plusieurs programmes ou bancs d'essais.

L'acheteur arrête sa décision selon les modalités précisées à l'article 9.10 du CCAP. Si la décision de vérification d'aptitude est positive, la vérification de service régulier débute.

8.4. La vérification de service régulier a pour objet de constater que les prestations fournies sont capables d'assurer un service régulier dans les conditions normales d'exploitation prévues dans les documents particuliers du marché.

La régularité du service s'observe pendant trente jours, à partir du jour de la décision positive de vérification d'aptitude prise par l'acheteur.

Le service est réputé régulier si la durée cumulée, sur le mois, des indisponibilités imputables à chaque élément ne dépasse pas 2 % de la durée d'utilisation effective (stations-services 7j/7, 24h/24).

L'acheteur arrête sa décision selon les modalités précisées à l'article 9.10 du CCAP.

## Article 9 - GARANTIE

9.1. Garantie de conformité des logiciels standards et des développements spécifiques :

Le titulaire garantit la conformité des logiciels standards aux spécifications prévues par les documents particuliers du marché.

A ce titre, pendant la durée de garantie, le titulaire corrige gratuitement toute anomalie de fonctionnement de son logiciel par rapport à aux spécifications du marché.

Lorsque l'anomalie est constatée sur un logiciel standard dont le titulaire n'est pas l'éditeur, le titulaire met en œuvre les clauses de garantie prévues par l'éditeur du logiciel standard concerné qui sont préalablement portées à la connaissance de l'acheteur. La correction est effectuée gratuitement.

Pour l'application du présent article, l'acheteur établit un compte rendu écrit de ces anomalies en donnant tous les éléments nécessaires à leur identification par le titulaire. Ce compte rendu doit être porté à la connaissance du titulaire dès la constatation de l'anomalie par l'acheteur.

9.2. Logiciels libres :

Les logiciels libres sont utilisés en l'état.

Le titulaire n'est pas responsable des dommages qui pourraient être causés par l'utilisation, par l'acheteur, de logiciels libres dont il n'est pas l'éditeur.

## Article 10 - MAINTENANCE, TIERCE MAINTENANCE APPLICATIVE

Par « maintenance », on désigne les prestations permettant le maintien en condition opérationnelle et le maintien en condition de sécurité des matériels à titre préventif, ou correctif.

Par « tierce maintenance applicative », on désigne les prestations qui consistent à conserver un système d'information dans un état lui permettant de remplir sa fonction. Ces prestations de maintien en condition opérationnelle et de maintien en condition de sécurité s'exécutent à titre préventif ou correctif. Elles peuvent également concerner des prestations d'évolution ou

d'adaptation des logiciels.

Ces services peuvent être rendus sur le site de l'acheteur ou à distance dans les locaux du titulaire en fonction des contraintes de sécurité liées à chaque type de prestation.

Des prestations de maintenance de matériel peuvent être incluses dans un marché de tierce maintenance applicative.

Par « préventif », on entend les mesures d'entretien exécutées pour éviter la survenance d'anomalies.

Par « correctif », on entend les mesures consistant à corriger les anomalies.

Par « évolutif », on entend les mesures de maintenance visant à faire évoluer une ou plusieurs applications, afin d'intégrer de nouvelles fonctions, d'en améliorer le fonctionnement et l'ergonomie ou de prendre en compte de nouvelles dispositions législatives ou réglementaires.

Par « adaptatif », on entend les mesures d'entretien et de maintenance permettant d'absorber des modifications de l'environnement technique d'exécution, comme les mises à jour ou les changements de systèmes d'exploitation, de bases de données, d'interfaces d'échange ou plus généralement des composants techniques et bibliothèques logicielles.

#### Article 11 - STIPULATIONS COMMUNES

Pour permettre à l'acheteur d'exercer les droits qui lui sont accordés au titre du marché, le titulaire livre spontanément et au fur et à mesure de l'exécution des prestations, l'ensemble des éléments nécessaires à cet exercice, ainsi que leurs mises à jour ou évolutions au cours du marché, tels que les licences, ou autres éléments nécessaires.