



**MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS**

*Liberté
Égalité
Fraternité*

**Direction du Renseignement et
de la Sécurité de la Défense**

Cahier des clauses techniques particulières (CCTP)

Prestations de formations dans le domaine
de la sécurité informatique au profit d'une entité du ministère
des Armées et des Anciens combattants

TABLE DES MATIÈRES

ARTICLE 1 – GÉNÉRALITÉS.....	3
1.1 - Objet de la consultation.....	3
1.2 - Justificatif du besoin	3
ARTICLE 2 – MODALITÉS D'EXÉCUTION DES PRESTATIONS.....	3
2.1 - Objectifs des formations	3
2.2 - Public visé	4
2.3 – Type de formation	4
2.4 - Lieu des prestations de formation	4
2.5 - Équipements nécessaires aux formations.....	4
2.6 - Logiciels, droits d'usage des logiciels.....	4
2.7 - Méthodologie et supports	5
2.8 - Langue de formation	5
2.9 - Composition des groupes de stagiaires.....	5
2.10 - Organisation et planification des formations	5
2.11 - Délai de réactivité du titulaire	5
ARTICLE 3 – ATTENTES DE L'ADMINISTRATION.....	6
3.1 - Confidentialité et discrétion	6
3.2 – Point de contact	6
3.3 - Qualité et contrôle des formations	6
3.4 - Obligations des formateurs.....	7
3.5 - Attestations de présence.....	7
3.6 - Documentation pédagogique	7
ARTICLE 4 – DISPOSITIFS D'ÉVALUATION.....	7
ARTICLE 5 – ÉVOLUTIONS DE LA PRESTATION.....	7
ANNEXE – FORMATIONS (sécurité systèmes et réseaux).....	9

ARTICLE 1 – GÉNÉRALITÉS

1.1 - Objet de la consultation

Le présent document constitue le Cahier des Clauses Techniques Particulières (CCTP) relatif aux prestations de formations dans le domaine de la sécurité informatique.

Il a pour objectif de décrire les prestations attendues du titulaire.

1.2 - Justificatif du besoin

Le ministère des Armées et des Anciens combattants souhaite mettre en place pour ses agents des formations dans le domaine de la sécurité informatique et ainsi amener son personnel à acquérir les niveaux de compétences nécessaires pour exercer leurs fonctions.

Le titulaire conçoit les contenus techniques et pédagogiques des modules de formation, en respectant les principes suivants :

- Les programmes sont conçus en prenant en compte des besoins exprimés par la personne publique ;
- Les contenus proposés sont conformes aux dispositions réglementaires (nationales et/ou internationales) ou normatives (certifications) : le titulaire s'engage à mettre à jour le contenu des modules de formation conformément aux évolutions réglementaires et/ou techniques.

Il est également demandé au titulaire de pouvoir réaliser, lorsque la personne publique lui demande, une formation « sur devis » respectant l'objet du marché. Le titulaire doit être en mesure de proposer un devis dans les 7 jours ouvrés suivant la demande de l'Administration sous peine de s'exposer aux pénalités prévues à l'article 9.3 du C.C.A.P.

Il est également demandé au titulaire de pouvoir proposer des certifications et éventuellement des cycles préparatoires spécifiques.

Enfin, le titulaire est en mesure de proposer une solution de formations en e-learning.

ARTICLE 2 – MODALITÉS D'EXÉCUTION DES PRESTATIONS

2.1 - Objectifs des formations

Les objectifs propres à chaque domaine de formation sont définis dans le tableau en annexe.

À l'issue de ces formations les stagiaires doivent être capables :

- dans le cadre d'un stage "niveau 1", de maîtriser les fonctionnalités du logiciel sur au moins un module ;
- dans le cadre d'un stage "niveau 2", de maîtriser le logiciel sur l'ensemble des modules.

2.2 - Public visé

Les prestations de formations sont organisées au profit des personnels civils et militaires d'une entité du ministère des Armées et des Anciens combattants.

2.3 – Type de formation

Les formations sont en **présentiel** ou en distanciel.

Les prestations de formation sont réalisées :

Soit en intra-entreprises :

La session concerne dans ce cas uniquement le personnel de l'entité du ministère des Armées et des anciens combattants.

Soit en inter-entreprises :

La session concerne quelques stagiaires de l'entité du ministère des Armées et des anciens combattants ainsi que du personnel relevant d'autres Administrations ou entreprises.

2.4 - Lieu des prestations de formation

Pour les formations en présentiel, les prestations de formation sont réalisées **dans les locaux du titulaire**.

Les repas sont inclus dans le coût de toute prestation impliquant des personnels de l'Administration.

2.5 - Équipements nécessaires aux formations

Formations inter-entreprises et intra-entreprises.

Le titulaire met à disposition des stagiaires l'ensemble des moyens nécessaires au déroulement de la prestation.

Chaque stagiaire doit disposer d'un poste de travail individuel pour les formations en présentiel.

2.6 - Logiciels, droits d'usage des logiciels

De manière générale, les formations portent sur la dernière version du logiciel. Le titulaire met ses cours et ses supports à jour, au fur et à mesure des changements de version. Toutefois, la personne publique se réserve la possibilité de commander des formations pour des logiciels dont la version n'est pas récente.

Par ailleurs, tous les types de supports utilisés au cours des formations (logiciels, documentation) doivent respecter la réglementation applicable en matière d'usage.

2.7 - Méthodologie et supports

Les formations associent des apports théoriques et méthodologiques selon les domaines abordés. Les formations doivent comporter, pour chaque domaine, une majorité de mises en pratique.

Le titulaire remet aux stagiaires des supports pédagogiques et pistes d'approfondissement (bibliographie, sites internet, etc.). Le prestataire utilise le système d'exploitation ou logiciel demandé par la personne publique.

2.8 - Langue de formation

Les formations ainsi que les supports sont délivrés en langue française. Néanmoins, à titre exceptionnel, et après autorisation, l'entité du ministère des Armées et des Anciens combattants peut accepter, pour certains niveaux de formation, des supports en langue anglaise.

2.9 - Composition des groupes de stagiaires

Le titulaire détermine le nombre minimal et maximal de stagiaires par session de stage, celui-ci ne pouvant être supérieur à douze (12) personnes.

2.10 - Organisation et planification des formations

L'organisation des formations fait l'objet d'une planification.

L'Administration et le titulaire désignent chacun un interlocuteur unique qui coordonne le déroulement de la prestation de la formation (planification des horaires, modalités d'organisation du stage, suivi de la commande...). La division formation-instruction (DFI) est l'interlocutrice technique du marché.

Un interlocuteur est désigné par le titulaire pour traiter les planifications, modalités pratiques de mise en formation, le suivi des commandes et tout incident rencontré.

La constitution des groupes de stagiaires est effectuée par DFI.

Dès la notification, la DFI organise avec le titulaire une réunion de cadrage pour le lancement du marché.

Par ailleurs, une réunion en présentiel ou en visio-conférence de planification annuelle est mise en place.

2.11 - Délai de réactivité du titulaire

À partir de la réception du bon de commande, le titulaire peut signaler par écrit son désaccord dans un délai de cinq (5) jours conformément à l'article 5.2 du CCAP.

2.11.1 Annulation ou report de session

Formation annulée ou reportée par le titulaire

En cas d'annulation ou de report du fait du titulaire, celui-ci doit informer l'Administration dans un délai de quinze (15) jours avant la date de début du stage. Les pénalités sont définies selon le CCAP.

Formation annulée ou reportée par l'Administration

L'Administration peut prononcer, pour des contraintes impérieuses de service, une annulation dans un délai de dix (10) jours avant la date de début du stage. Le stage peut faire l'objet d'un report à une date ultérieure convenue entre les deux parties.

2.11.2 Absence du/des formateur (s)

Le titulaire prend toutes les dispositions nécessaires pour assurer la continuité du service en cas d'absence des formateurs, en proposant des remplaçants aux profils similaires.

2.11.3 Convocations

Le prestataire notifie par courriel quinze (15) jours au plus tard avant le démarrage de la formation, les informations suivantes : convocation nominative et plan d'accès.

ARTICLE 3 – ATTENTES DE L'ADMINISTRATION

3.1 - Confidentialité et discrétion

Conformément à l'article 413-13 du code pénal, le titulaire s'engage à ne révéler aucune information qui pourrait conduire, directement ou indirectement, à la découverte de l'identité d'un agent d'un service mentionné à l'article L. 811-2 du code de la sécurité intérieure ou de son appartenance à l'un de ces services.

L'identité des stagiaires n'est pas mentionnée sur les factures et l'appartenance à l'un de ces services n'apparaît pas sur les documents ou supports relatifs à la formation. Enfin, le titulaire met en place toutes les procédures nécessaires pour garantir l'anonymat des stagiaires et ne fait aucune mention du présent marché dans ses listes de référence ou auprès d'entreprises, associations tierces ou partenaires.

Les principes de confidentialité et de discrétion sont valables pour le titulaire, son personnel, ses formateurs et sous-traitants.

3.2 – Point de contact

Le titulaire doit obligatoirement désigner un référent ainsi qu'un suppléant afin de faciliter tout échange avec l'Administration relatif à la mise en place d'une formation.

3.3 - Qualité et contrôle des formations

Le titulaire respecte son engagement qualité et son processus de qualification des formateurs détaillés dans son offre technique. Il est tenu de réaliser sa prestation selon les prescriptions du marché. En cas de non-respect de cette obligation, l'Administration lui demande de procéder aux réajustements nécessaires soit au cours de la session, soit pour les sessions à venir c'est-à-dire de recommencer la prestation, à ses frais, selon les modalités initialement prévues. Pour les problèmes

relevant de sa responsabilité, le titulaire met tout en œuvre pour apporter une solution corrective.

3.4 - Obligations des formateurs

Le formateur s'engage à respecter les spécificités de la formation, ses objectifs pédagogiques ainsi que la totalité de son contenu, de ses thématiques et du programme.

3.5 - Attestations de présence

Le titulaire constitue les feuilles d'émargement par journée pendant toute la durée de la formation. Il transmet ces documents à la personne publique dans les huit (8) jours suivant la date de la fin de la formation. En fin de stage, le titulaire remet à chaque stagiaire une attestation nominative de stage.

3.6 - Documentation pédagogique

L'élaboration et la fourniture de la documentation pédagogique sont à la charge du titulaire.

ARTICLE 4 – DISPOSITIFS D'ÉVALUATION

En fin de formation, l'intervenant fait remplir à chaque stagiaire une fiche d'évaluation « à chaud » de la prestation.

Ces évaluations sont envoyées scannées par voie électronique au représentant de la personne publique dans un délai de dix (10) jours.

L'Administration se réserve le droit de désigner un représentant qualifié afin d'assister ponctuellement à des séances de formation.

ARTICLE 5 – ÉVOLUTIONS DE LA PRESTATION

L'offre doit pouvoir évoluer pendant la durée du contrat en fonction des évolutions sociétales et technologiques ainsi que des retours d'expérience. Le titulaire propose à son initiative une évolution de son offre susceptible d'apporter une plus-value technique ou commerciale, notamment des améliorations des prestations consécutives à des corrections d'anomalies ou des modifications de programmes pédagogiques. L'Administration doit être informée par le titulaire, au préalable, de toute évolution ou modification importante pouvant avoir un impact technique sur la solution proposée.

Un point de situation annuel est effectué entre la Division Formation-Instruction et le titulaire du marché.

ANNEXE – Formations

Sécurité systèmes et réseaux			
POSTE	INTITULE	NIVEAU	DESCRIPTION
1	Sécurité réseau	Niveau 1	→ description des menaces pesant sur la sécurité des réseaux → gestion des risques internes et externes liés à l'utilisation d'internet : bonnes pratiques techniques/organisationnelles pour renforcer la sécurité des réseaux
2	Sécurité réseau	Niveau 2	→ Maîtrise de la sécurisation des réseaux interconnectés avec Internet → sécurisation des réseaux privés utilisant les technologies internet/intranet et de leurs interconnexions avec des réseaux extérieurs
3	Sécurité web et intrusions	Niveau 1	→ problématiques et enjeux sur la sécurité web → évolution des attaques et parades associées → fondamentaux pour protéger un serveur Web / une application
4	Sécurité web et intrusions	Niveau 2	Maîtriser la sécurité du web et de l'internet → défense contre les intrusions réseau → faille des navigateurs et des réseaux sociaux → solutions pour protéger ses applications
5	Détection d'intrusions	Niveau 1	→ présentation des techniques d'intrusion et des principales attaques et du panel d'outils permettant d'y faire face → différences entre IDS et IPS et avantages comparés
6	Détection d'intrusions	Niveau 2	→ Comprendre et mettre en œuvre des techniques d'intrusion → Attaques réseaux, vulnérabilités web avancées, cryptographie par la pratique
7	La VoIP	Niveau 1	→ Découvrir les fondamentaux de la VoIP → la VoIP : configuration
8	La VoIP	Niveau 2	→ sécurité (implémentation et encryptage) et menaces (hacking de la VoIP) → la VoIP : configuration avancée et sécurisée

9	Audit et analyse des réseaux	Niveau 1	Être capable de mener un audit de résolution de panne et de sécurité selon : → une méthodologie et des outils d'audit → les architectures de réseaux d'entreprise→ des outils de métrologie → la gestion du trafic → la mise en œuvre de mécanismes de sécurité
10	Audit et analyse des réseaux	Niveau 2	→ optimiser la performance du réseau d'entreprise sur les aspects sécurité et qualité de service→ mettre en œuvre des outils d'audit et de qualité de service
11	Sécurité Windows : postes de travail	Niveau 1	→ Mécanismes de sécurité des environnements Windows 10 et 11 → sécurité de base du système → sécurité des fonctionnalités réseau et applicatives
12	Sécurité Windows : serveurs	Niveau 2	→ fonctionnalités de sécurité d'une architecture Windows serveur 2019/2016 → déploiement d'une PKI → déploiement et sécurisation d'un AD → sécurisation avancée : VPN et IPSec
13	Sécurité des informations dans le cloud	/	→ analyse des menaces et vulnérabilités → fondamentaux de la sécurité dans le Cloud → protection des données dans le Cloud → moyens de contrôle du fournisseur
14	Formation sur devis	/	L'Administration se réserve le droit de solliciter une prestation de formation non détaillée actuellement dans le présent marché. Ce type de formation est satisfait par devis en application de l'article 1.2. du présent document.

Glossaire des sigles précisés dans la présente annexe

AD : Active directory (service d'annuaire)

IDS : intrusion detection system (système de détection d'intrusion)

IPS : Intrusion prévention system (système de prévention d'intrusion)

PKI : Public key infrastructure (infrastructure à clés publiques)

VoIP : Voice over internet protocol (la voix sur IP)

VPN : Virtual private network (réseau privé virtuel)