Protégez vos données sensibles ou classifiées

Des formations destinées aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

- Réforme de la protection du secret : évolutions de l'instruction générale interministérielle 1300 (IGI 1300) et son application pratique dans l'entreprise
- Formation des officiers de sécurité (OS)
- Dirigeants d'entreprise : appréhender de futurs marchés avec accès ou détention d'informations et supports classifiés
- Collaborateurs d'entreprise : connaître les exigences liées aux informations classifiées
- Identification et gestion des données sensibles au sein de votre entreprise

Des dispositifs d'accompagnement destinés à aligner les comportements de vos collaborateurs sur vos dispositifs de protection des données sensibles

- Data Shield® : instaurer une culture de protection des données auprès des collaborateurs
- Sécuriser la gestion des départs de vos collaborateurs dans le cadre de la protection de vos données sensibles

Pour aller plus loin…

Modification des dispositions réglementaires relatives aux modalités de classification et de protection du secret de la défense nationale

Aujourd'hui, près de 400.000 personnes ont accès à des informations classifiées, soit 0,6 % des Français. Les habilitations sont accordées pour 70 % à du personnel du ministère des Armées. Fin 2017, la France a entrepris de réformer les niveaux de protection des informations classifiées : au 1er juillet 2021, seuls deux subsisteront (« secret » et « très secret »), le niveau « confidentiel défense » étant supprimé.

Le niveau « secret » sera réservé aux informations et supports dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale. Le niveau « très secret » lui sera réservé aux informations et supports dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale.

Cette réforme s'effectue dans le cadre d'une nouvelle édition de l'instruction générale interministérielle sur la protection du secret de la défense et de la sécurité nationale n° 1300 (IGI 1300) menée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

L'objectif est à la fois d'éviter une inflation inutile de données classifiées, d'atteindre une protection encore plus efficace et de faciliter les échanges avec nos principaux partenaires étrangers.

Protection du secret de la défense nationale et PPST : des dispositifs complémentaires

La protection du secret de la défense nationale vise à protéger des informations et des supports classifiés (ISC) de toute compromission. La protection du potentiel scientifique et technique de la nation (PPST) a pour but, elle, la protection des savoir-faire nationaux. Ainsi, les régimes de contrôles d'accès sont différents. Les enquêtes administratives menées dans le cadre de la protection du secret (pour une habilitation, ou pour l'accès à une zone réservée, par exemple) détectent les vulnérabilités des personnes physiques ou morales. Les contrôles effectués au titre des zones à régime restrictif (ZRR) dans le cadre de la PPST, quant à eux, prennent en compte le risque que représentent les personnes physiques au regard de leur pays d'appartenance et de la nature des activités exercées au sein de la ZRR.

Dispositif Data Shield®

« Notre programme Data Shield® est totalement complémentaire aux actions menées par les RSSI/DSI. Il permet de vérifier que les comportements des collaborateurs sont alignés sur la stratégie générale de sécurité de l'entreprise. Nous travaillons en très étroite coopération avec eux en permettant de déceler des failles, voire les zones à risques, tant dans le domaine du comportement que de l'organisation. Le fait de mettre à jour tous les comportements à risques, et non seulement ceux liés à l'utilisation des systèmes d'information, leur permet d'avoir une vue plus globale de la mise en application des dispositifs de sécurité et de mettre à jour les pratiques non détectées par les dispositifs traditionnels. »

Extrait de l'interview de Pascaline Abdini, directrice générale du cabinet Cluster Défense Sécurité, publié dans le dernier numéro du Livre Blanc d'Ercom « Protection des données : pourquoi et comment RSSI et DSI doivent-ils collaborer ? ». Filiale du groupe THALES, Ercom développe une gamme complète de solutions pour lutter contre le hacking des terminaux et le piratage des communications et des données. Ercom sécurise notamment les 20.000 terminaux du ministère des Armées à l'aide de sa solution Cryptosmart.

Formation destinée aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

FORMATIONS

Intitulé :	**Réforme de la protection du secret : évolutions de l'instruction générale interministérielle 1300 (IGI 1300) et son application pratique dans l'entreprise**
Pour qui :	Officiers de sécurité (OS). Officiers de sécurité des systèmes d'information (OSSI). Directeurs sûreté. Collaborateurs gérant des informations et supports classifiés (ISC) au sein d'une entreprise.
Enjeu :	Anticiper la mise en œuvre dans votre entreprise de la nouvelle réglementation de la protection du secret de la défense nationale.
Prérequis :	Connaissances de base dans le domaine de la protection du secret.
Objectifs :	Identifier les nouvelles dispositions de l'IGI 1300. Optimiser les processus d'habilitation au sein de votre entreprise. Mieux intégrer la protection des informations dématérialisées.
Programme :	Les habilitations (personnes physiques et morales). La protection du secret dans les contrats. La gestion des ISC. Les dispositions relatives aux systèmes d'information classifiés. La protection des lieux abritant. Les compromissions.
Points forts/moyens pédagogiques :	Formation dispensée par un expert, ancien fonctionnaire sécurité-défense (FSD) d'un ministère régalien ayant été l'un des principaux contributeurs de la rédaction de la nouvelle réglementation sur la protection du secret de la défense nationale. Echanges de pratiques et retours d'expérience.
Modalités :	Durée 1 jour. Formation inter-entreprises. 8 à 15 personnes. La formation se déroule dans le centre de Paris dans des locaux facilement accessibles (métro et navettes aéroports notamment). Accueil café et déjeuner sur place inclus.
Montant :	1.150 € net de taxes par personne.
Code formation :	IGI/2020/FS
Informations complémentaires :	Cette formation peut être réalisée en intra-entreprise sur demande. Elle ne se substitue pas aux échanges avec les services spécialisés du ministère de l'Intérieur ou du ministère des Armées.

Formation destinée aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

FORMATIONS

Intitulé :	**Formation des officiers de sécurité**
Pour qui :	Officiers de sécurité (OS) futurs OS et leurs collaborateurs. Directeurs sûreté, responsables sûreté et leurs collaborateurs.
Enjeu :	Renforcer la protection des informations et des installations sensibles de l'entreprise, sachant que les nouvelles dispositions de l'IGI 1300 précisent que l'officier de sécurité doit être formé à la législation et à la réglementation relatives à la protection du secret de la défense nationale.
Prérequis :	Avoir un poste en relation avec la protection des informations et/ou des installations.
Objectifs :	Acquérir des connaissances et des outils pour assurer la protection des informations (sensibles ou classifiées) et des installations de votre entreprise.
Programme :	Module « Protection du secret » (habilitations, protection du secret dans les contrats…). Module « Protection des informations sensibles » (PPST, RGPD, dispositions relatives aux systèmes d'information…). Module « Protection physique des installations » (analyse des risques, protection des lieux abritant…). Module « L'humain au cœur de la protection » (facteurs de risques, comportements et organisation).
Points forts/moyens pédagogiques :	Formation dispensée par des intervenants ayant des expertises complémentaires et une expérience avérée (ancien fonctionnaire sécurité-défense d'un ministère régalien, consultante spécialisée dans les comportements humains au sein des organisations). Formation prenant en compte les évolutions de la réglementation en matière de protection du secret (IGI 1300). Echanges de pratiques et retours d'expérience.
Modalités :	Durée 3 jours. Formation inter-entreprises. 8 à 15 personnes. La formation se déroule dans le centre de Paris dans des locaux facilement accessibles (métro et navettes aéroports notamment). Accueil café et déjeuner sur place inclus durant les 3 jours de la formation.
Montant :	2.350 € net de taxes par personne.
Code formation :	OS/2020/FS
Informations complémentaires :	Cette formation peut être réalisée en intra-entreprise sur demande. Elle ne se substitue pas aux échanges avec les services spécialisés du ministère de l'Intérieur ou du ministère des Armées.

Formation destinée aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

FORMATIONS

Intitulé :	**Dirigeants d'entreprise : appréhender de futurs marchés avec accès ou détention d'informations et supports classifiés**
Pour qui :	Dirigeants d'entreprise. Directeurs R & D. Directeurs commerciaux. Directeurs de « business unit ». Etc.
Enjeu :	Votre entreprise va accéder à des marchés nécessitant l'accès ou la détention d'informations et supports classifiés (ISC). Cette formation a pour but vous de donner une vue la plus complète et la plus claire possible des enjeux - notamment les responsabilités contractuelles et pénales - et de les anticiper au mieux.
Prérequis :	Aucun.
Objectifs :	Comprendre la notion de protection du secret. Faire le lien avec les marchés entraînant l'accès ou la détention d'informations et supports classifiés (ISC). Bien identifier les responsabilités liées à ces marchés pour votre entreprise et les anticiper au mieux.
Programme :	Les principes généraux de la protection du secret. Les habilitations (personnes physiques et morales). La protection du secret dans les contrats. L'entreprise et la gestion des informations et supports classifiés.
Points forts/moyens pédagogiques :	Formation dispensée par un expert de la protection du secret de la défense nationale ayant en parallèle une très large expérience du monde de l'entreprise, notamment dans le secteur aéronautique, défense et sécurité.
Modalités :	Durée 1/2 journée. Formation inter-entreprises. 8 à 15 personnes. La formation se déroule dans le centre de Paris dans des locaux facilement accessibles (métro et navettes aéroports notamment). Accueil café inclus.
Montant :	850 € net de taxes par personne.
Code formation :	DR/2020/FS
Informations complémentaires :	Cette formation peut être réalisée en intra-entreprise sur demande. Elle ne se substitue pas aux échanges avec les services spécialisés du ministère de l'Intérieur ou du ministère des Armées.

Formation destinée aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

FORMATIONS

Intitulé :	**Collaborateurs d'entreprise : connaître les exigences liées aux informations classifiées**
Pour qui :	Collaborateurs (consultants, commerciaux, techniciens...) ayant à connaître des informations classifiées au titre de l'exécution d'un contrat.
Enjeu :	Des collaborateurs de votre entreprise ont ou vont avoir accès à des informations classifiées au titre de l'exécution d'un contrat. Cette formation a pour but de les préparer à exercer ces responsabilités.
Prérequis :	Aucun.
Objectifs :	Comprendre la notion de protection du secret et ses implications dans l'accès ou la détention d'informations et supports classifiés (ISC) dans le cadre d'un contrat. Appréhender les responsabilités contractuelles et pénales pour les collaborateurs concernés et l'entreprise. Connaître et mettre en pratique les bons comportements dans le cadre de la protection du secret.
Programme :	La protection du secret : présentation générale. Les habilitations et la protection du secret dans les contrats. Votre entreprise et la gestion des informations et supports classifiés. La responsabilité du collaborateur dans le cadre de la protection du secret. Adopter les bons comportements dans le cadre de la protection du secret.
Points forts/moyens pédagogiques :	Formation dispensée par un expert de la protection du secret de la défense nationale ayant en parallèle une très large expérience du monde de l'entreprise, notamment dans le secteur aéronautique, défense et sécurité. Echanges de pratiques et retours d'expérience.
Modalités :	Durée 1/2 journée. Formation inter-entreprises. 8 à 15 personnes. La formation se déroule dans le centre de Paris dans des locaux facilement accessibles (métro et navettes aéroports notamment). Accueil café inclus.
Montant :	750 € net de taxes par personne.
Code formation :	CO/2020/FS
Informations complémentaires :	Cette formation peut être réalisée en intra-entreprise sur demande. Elle ne se substitue pas aux échanges avec les services spécialisés du ministère de l'Intérieur ou du ministère des Armées.

Formation destinée aux experts de la sécurité de l'information et de la protection des données sensibles ou classifiées

FORMATIONS

Intitulé :	**Identification et gestion des données sensibles au sein de votre entreprise**
Pour qui :	Direction générale. Directeurs commerciaux. Directeurs R & D. Directeurs de « Business Unit ». DPO. Etc.
Enjeu :	Identifier les informations sensibles de votre entreprise et mettre en place un dispositif adapté pour en assurer la protection.
Prérequis :	Aucun.
Objectifs :	Identifier les informations sensibles de votre entreprise. Connaître les dispositifs réglementaires de protection. Informer et impliquer vos collaborateurs.
Programme :	Critères de définition d'une information sensible. Identification des informations à protéger. Dispositifs de protection possibles. Comment impliquer vos collaborateurs. Exemple d'application pratique.
Points forts/moyens pédagogiques :	Formation illustrée par un cas pratique qui servira de fil rouge pour mieux appréhender la mise en place opérationnelle de la protection d'informations et de données sensibles au sein de votre entreprise. Formation dispensée par des intervenants ayant des expertises complémentaires (protection des informations y compris dans le domaine régalien, comportements humains…) sur les thèmes abordés.
Modalités :	Durée 1 jour. Formation en inter-entreprises. 8 à 15 personnes. La formation se déroule dans le centre de Paris dans des locaux facilement accessibles (métro et navettes aéroports notamment). Accueil café et déjeuner sur place inclus.
Montant :	1.050 € net de taxes par personne.
Code formation :	GS/2020/FS
Informations complémentaires :	Cette formation peut être réalisée en intra-entreprise sur demande. Elle peut être complétée par un accompagnement dédié pour vous permettre de mettre en place un dispositif adapté de protection des données sensibles au sein de votre entreprise et en assurer le suivi en liaison étroite avec les collaborateurs concernés.

Dispositifs d'accompagnement destinés à aligner les comportements de vos collaborateurs sur vos dispositifs de protection des données sensibles

ACCOMPAGNEMENTS

Data Shield®
Instaurer une culture de protection des données auprès des collaborateurs

Data Shield® permet aux collaborateurs de :

- Prendre conscience des enjeux et des risques liés à la protection des données sensibles.
- Mettre à jour les comportements qui peuvent s'avérer à risques.
- Mettre à jour les bonnes pratiques, tant au niveau organisationnel que des comportements, y compris hors entreprise (réseaux sociaux…).

Data Shield® permet aux RSSI, DSI, DPO et à la direction générale :

- D'avoir une vue d'ensemble de la mise en application ou non par les collaborateurs des différents dispositifs de sécurité/sûreté.
- Mettre à jour les pratiques à risques non détectées par les dispositifs traditionnels.
- Aligner les comportements sur la stratégie de sécurité globale de l'entreprise.

Les + de Data Shield® :

- Programme conçu sur mesure en fonction du secteur d'activité, de la réglementation et de la législation en vigueur.
- S'intègre dans les dispositifs existants et en optimise l'efficience.
- Méthodologie reposant sur des échanges constructifs qui favorisent l'intelligence collective et l'adhésion des participants.
- Conçu et animé par deux experts, l'un dans le domaine des comportements humains et l'autre dans celui de la protection des données.

1	2	3	4	5
Diagnostic : Analyse des besoins et des enjeux avec les parties prenantes	Elaborer une formation sur mesure	Préparer les interventions et réaliser les sessions auprès des collaborateurs	Synthèse et restitution de la formation et des plans d'action auprès des parties prenantes	Assurer le suivi des plans d'action et la mise en place d'un dispositif de détection des signaux faibles

Ce dispositif comprend des modules de conseil et de formation. Il est élaboré sur mesure et mis en place exclusivement en intra-entreprise. Pour en savoir plus et organiser une éventuelle présentation au sein de votre entreprise :

Pascaline Abdini
p.abdini@clusterdefensesecurite.fr
+33 6 08 81 17 08

ACCOMPAGNEMENTS

Sécuriser la gestion des départs de vos collaborateurs dans le cadre de la protection de vos données sensibles

La gestion des départs est un sujet central de la sécurité des données sensibles de votre entreprise.

Si les comportements humains constituent une composante majeure des dispositifs de sécurité, ils deviennent encore plus sensibles lorsque votre entreprise est en phase de licenciement.

Les collaborateurs, par déception, voire par esprit de vengeance, peuvent nuire à l'image de votre entreprise, mais surtout peuvent détruire ou partir avec des données sensibles ou diffuser des informations confidentielles.

Plus les personnes s'estiment injustement traitées, ou bien ont le sentiment de quitter l'entreprise en n'ayant ni considération ni reconnaissance, et plus elles peuvent être enclines à ce type de comportement.

Cible : Les collaborateurs amenés à quitter l'entreprise.


DR

Objectifs :

- Leur permettre de prendre conscience des points positifs de leur expérience professionnelle au sein de votre entreprise.
- Valoriser leurs acquis professionnels.
- Mettre à jour les savoir-être et les savoir-faire acquis.
- Les accompagner pour se positionner sur un nouveau projet professionnel.

Les + de ce programme :

- Programme défini en collaboration avec le DRH, RSSI, DSI, DPO…
- Programme construit « sur mesure » en fonction des spécificités de l'entreprise et du profil des collaborateurs concernés.

Pour en savoir plus et organiser une éventuelle présentation au sein de votre entreprise :
Pascaline Abdini
p.abdini@clusterdefensesecurite.fr
+33 6 08 81 17 08

Planning prévisionnel des formations inter-entreprises

Paris

Premier semestre 2020	Avril	Mai	Juin	Juillet
Réforme de la protection du secret : évolutions de l'instruction générale interministérielle 1300 (IGI 1300) 1 jour		12 mai 13 mai	9 juin 10 juin	8 juillet 9 juillet
Formation des officiers de sécurité (OS) 3 jours		26, 27 et 28 mai	16, 17 et 18 juin	
Dirigeants d'entreprise : appréhender de futurs marchés avec accès ou détention d'informations et supports classifiés ½ journée	16 avril matin		19 juin matin	
Collaborateurs d'entreprise : connaître les exigences liées aux informations classifiées ½ journée	16 avril après-midi		19 juin après-midi	
Identification et gestion des données sensibles au sein de votre entreprise 1 jour	15 avril		11 juin	22 juillet

Second semestre 2020	Septembre	Octobre	Novembre	Décembre
Réforme de la protection du secret : évolutions de l'instruction générale interministérielle 1300 (IGI 1300) 1 jour	9 septembre 10 septembre	6 octobre 7 octobre	4 novembre 5 novembre	8 décembre 9 décembre 10 décembre
Formation des officiers de sécurité (OS) 3 jours	22, 23 et 24 septembre	13, 14 et 15 octobre	24, 25 et 26 novembre	
Dirigeants d'entreprise : appréhender de futurs marchés avec accès ou détention d'informations et supports classifiés ½ journée		8 octobre matin		3 décembre matin
Collaborateurs d'entreprise : connaître les exigences liées aux informations classifiées ½ journée		8 octobre après-midi		3 décembre après-midi
Identification et gestion des données sensibles au sein de votre entreprise 1 jour	15 septembre			

Le cabinet Cluster Défense Sécurité anime deux groupes sur LinkedIn :

« **Protection des informations sensibles et du Secret** » et « **Comportements humains et protection des données** ».

Pour demander à les rejoindre :

Protection des informations sensibles et du Secret

Comportements humains et protection des données

Bon de commande
INSCRIPTION À UNE FORMATION

Pascaline Abdini
p.abdini@clusterdefensesecurite.fr
+33 (0)6 08 81 17 08

STAGE

Intitulé . . . . . .

Référence |__|__|__|__|__| Date . . . . / . . . . / . . . . Lieu : Paris

Montant net de taxes . . . . . € (accueil-café et déjeuner inclus pour les formations d'une journée, accueil-café inclus pour les formations d'une demi-journée)

Participant

☐ M. ☐ Mme Nom . . . . . Prénom . . . . .

Fonction . . . . . Téléphone (ligne directe) . . . . .

E. mail . . . . .

Entreprise ou organisme

Raison sociale . . . . . Adresse . . . . .

Code postal . . . . . Ville . . . . .

Siret |__|__|__|__|__|__|__|__|__|__|__|__|__|__| Code APE / NAF |__|__|__|

Responsable formation : Nom . . . . . Prénom . . . . .

Téléphone (ligne directe) . . . . . E.mail . . . . .

Facturation (à remplir impérativement au moment de l'inscription)

Prise en charge de la formation par un OPCO ☐ oui ☐ non

Si oui : envoi de la facture à l'OPCO :

Nom . . . . . Adresse . . . . .

Code postal . . . . . Ville . . . . .

Nom et Prénom de votre contact . . . . .

Téléphone (ligne directe) . . . . . E.mail . . . . .

Un accord de prise en charge de l'OPCO doit nous parvenir par courrier avant le début de la formation.
Dans le cas contraire, l'entreprise sera facturée sur l'intégralité de la formation.

Si non : envoi de la facture à l'entreprise.

Date : . . . . / . . . . / . . . . Signature précédée de la mention « bon pour accord » Cachet de la société

Pour les formations intra-entreprise réalisées hors de Paris, les frais supplémentaires (transport, repas, frais divers…) sont facturés à part avec les justificatifs.

La signature du présent bulletin vaut acceptation des conditions générales de vente.

Les informations recueillies dans le cadre du présent bulletin d'inscription font l'objet d'un traitement informatique par le cabinet Cluster Défense Sécurité à des fins de gestion des relations avec ses clients et prospects. Ces informations sont destinées uniquement au cabinet Cluster Défense Sécurité et ne sont ni revendues, ni louées ni prêtées. Conformément au Règlement général sur la protection des données (RGPD) vous avez la possibilité d'exercer votre droit à l'effacement (« droit à l'oubli ») en contactant par écrit le cabinet Cluster Défense Sécurité 115 rue Saint-Dominique 75007 Paris.

Conditions Générales de Vente
(Formation professionnelle continue)

1. PRESENTATION

Cluster Défense Sécurité est un organisme de formation professionnelle dont le siège social est établi au 115 rue Saint-Dominique 75007 Paris. Cluster Défense Sécurité développe, propose et dispense des formations en présentiel inter et intra-entreprise. L'ensemble des prestations Cluster Défense Sécurité est ci-après dénommé « Offre de formation Cluster Défense Sécurité ».

2. OBJET

Les présentes conditions générales de vente (ci-après dénommée « CGV ») s'appliquent à toutes les offres de formation Cluster Défense Sécurité relatives à des commandes passées auprès de Cluster Défense Sécurité par tout client professionnel (ci-après dénommé « le Client »). Le fait de passer commande implique l'adhésion entière et sans réserve du Client aux présentes CGV. Toute condition contraire et notamment toute condition générale ou particulière opposée par le Client ne peut, sauf acceptation formelle et écrite de Cluster Défense Sécurité, prévaloir sur les présentes CGV et ce, quel que soit le moment où elle aura pu être portée à sa connaissance. Le fait que Cluster Défense Sécurité ne se prévale pas à un moment donné de l'une quelconque des présentes CGV ne peut être interprété comme valant renonciation à s'en prévaloir ultérieurement. Le Client se porte fort du respect des présentes CGV par l'ensemble de ses salariés, préposés et agents. Le Client reconnaît également que, préalablement à toute commande, il a bénéficié des informations et conseils suffisants de la part de Cluster Défense Sécurité, lui permettant de s'assurer de l'adéquation de l'Offre de formation à ses besoins.

3. FORMATION EN PRESENTIEL

3.1 Formations en inter-entreprise

3.1.1 Descriptif. Les dispositions du présent article concernent les formations Inter-entreprises, disponibles au catalogue de Cluster Défense Sécurité et exécutées dans des locaux mis à disposition par Cluster Défense Sécurité.

3.1.2 Conformité des locaux mis à disposition par Cluster Défense Sécurité. Cluster Défense Sécurité s'engage à ce que les locaux :

- répondent aux normes ERP et soient accessibles aux personnes handicapées.
- permettent aux stagiaires de suivre la formation dans de bonnes conditions.

3.1.3 Conditions financières. Le règlement du prix de la formation est à effectuer, à l'inscription, comptant, sans escompte, à l'ordre de Cluster Défense Sécurité.

3.1.4 Abandon d'un participant. Tout stage commencé et non terminé par le client, pour toute raison autre qu'une maladie ou un accident est intégralement dû à Cluster Défense Sécurité.

3.1.5 Remplacement d'un participant. Cluster Défense Sécurité offre la possibilité de remplacer un participant empêché par un autre participant ayant le même profil et les mêmes besoins en formation.

3.1.6 Insuffisance du nombre de participants à une session. Dans le cas où le nombre de participants serait insuffisant pour assurer le bon déroulement de la session de formation, Cluster Défense Sécurité se réserve la possibilité d'ajourner la formation au plus tard une semaine avant la date prévue et ce, sans indemnités.

3.2 Formations intra-entreprise

3.2.1 Descriptif. Les dispositions du présent article concernent les formations intra-entreprise développées sur mesure et exécutées dans les locaux du client ou mis à disposition par le client. Lors de la formation sur le site client, la formation est en principe dispensée dans des locaux distincts des lieux de travail habituels des stagiaires conformément à l'article D6321-3 du Code du travail. Il appartient au client de respecter les articles D6321-1 et D6321-3 du Code du travail.

3.2.2. Conditions financières. Toute formation intra-entreprise fera préalablement l'objet d'une proposition commerciale et financière par Cluster Défense Sécurité. La facturation et le règlement se font à l'issue du stage. Sauf disposition contraire dans la proposition Cluster Défense Sécurité, un acompte minimum de 20 % du coût total de la formation sera versé par le client.

4. DISPOSITIONS COMMUNES AUX FORMATIONS

4.1 Documents contractuels. Pour chaque action de formation une convention établie selon les articles L 6353-1 et L 6353-2 du Code du travail est adressée en deux exemplaires dont un est à retourner par le Client revêtu du cachet de l'entreprise. L'attestation de participation est adressée après la formation. Une attestation de présence pour chaque partie peut être fournie sur demande.

4.2 Règlement par un OPCO. En cas de règlement par l'OPCO dont dépend le Client, il appartient au Client d'effectuer la demande de prise en charge avant le début de la formation auprès de l'OPCO. L'accord de financement doit être communiqué au moment de l'inscription et sur l'exemplaire de la convention que le Client retourne signé à Cluster Défense Sécurité. En cas de prise en charge partielle par l'OPCO, la différence sera directement facturée par Cluster Défense Sécurité au Client. Si l'accord de prise en charge de l'OPCO ne parvient pas à Cluster Défense Sécurité au premier jour de la formation, Cluster Défense Sécurité se réserve la possibilité de facturer la totalité des frais de formation au Client.

4.3 Annulation des formations en présentiel à l'initiative du Client. Les dates de formation en présentiel sont fixées d'un commun accord entre Cluster Défense Sécurité et le Client et sont bloquées de façon ferme. En cas d'annulation tardive par le Client d'une session de formation planifiée en commun, des indemnités compensatrices sont dues dans les conditions suivantes :

- report ou annulation communiqué au moins 30 jours calendaires avant la session : aucune indemnité.
- report ou annulation communiqué moins de 15 jours calendaires avant la session : totalité des honoraires relatifs à la session facturée au Client.

5. DISPOSITIONS APPLICABLES À L'OFFRE DE FORMATION CLUSTER DEFENSE SECURITE

5.1 Modalités de passation des commandes

La proposition et les prix indiqués par Cluster Défense Sécurité sont valables 2 mois à partir de la date de la proposition commerciale et financière. L'offre de formation est réputée acceptée dès la réception par Cluster Défense Sécurité d'un bon de commande ou d'un bulletin d'inscription signé par tout représentant dûment habilité du Client. La signature du bon de commande, du bulletin d'inscription et/ou l'accord sur proposition implique la connaissance et l'acceptation irrévocable et sans réserve des présentes conditions, lesquelles pourront être modifiées par Cluster Défense Sécurité à tout moment, sans préavis, et sans que cette modification ouvre droit à indemnité au profit du Client.

5.2. Facturation - Règlement

5.2.1 Prix. Tous les prix sont exprimés en euros et sont nets de taxes.

5.2.2 Paiement. Sauf convention contraire, les règlements seront effectués aux conditions suivantes : - le paiement comptant doit être effectué par le Client dès réception de la facture,- le règlement est accepté par chèque ou virement bancaire. Toute somme non payée à échéance entraîne de plein droit et sans mise en demeure préalable, l'application de pénalités d'un montant égal à trois fois le taux d'intérêt légal. Cluster Défense Sécurité aura la faculté de suspendre les prestations de formation jusqu'à complet paiement et obtenir le règlement par voie contentieuse aux frais du Client sans préjudice des autres dommages et intérêts qui pourraient être dus à Cluster Défense Sécurité.

5.3. Limitations de responsabilité de Cluster Défense Sécurité. La responsabilité de Cluster Défense Sécurité ne peut en aucun cas être engagée pour toute défaillance technique du matériel. Quel que soit le type de prestations, la responsabilité de Cluster Défense Sécurité est expressément limitée à l'indemnisation des dommages directs prouvés par le Client. En aucun cas, la responsabilité de Cluster Défense Sécurité ne saurait être engagée au titre des dommages indirects tels que perte de données, de fichier(s), perte d'exploitation, préjudice commercial, manque à gagner, atteinte à l'image et à la réputation.

5.4. Force majeure. Cluster Défense Sécurité ne pourra être tenue responsable à l'égard du Client en cas d'inexécution de ses obligations résultant d'un évènement de force majeure. Sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement reconnus par la jurisprudence des Cours et Tribunaux français et sans que cette liste soit restrictive : la maladie ou l'accident d'un consultant ou d'un animateur de formation, les grèves ou conflits sociaux internes ou externes à Cluster Défense Sécurité, les désastres naturels, les incendies, la non-obtention de visas, des autorisations de travail ou d'autres permis, les lois ou règlements mis en place ultérieurement, l'interruption des télécommunications, l'interruption de l'approvisionnement en énergie, l'interruption des communications ou des transports de tout type, ou toute autre circonstance échappant au contrôle raisonnable de Cluster Défense Sécurité.

5.5. Propriété intellectuelle. Cluster Défense Sécurité est seule titulaire des droits de propriété intellectuelle de l'ensemble des formations qu'elle propose à ses Clients. À cet effet, l'ensemble des contenus et supports pédagogiques quelle qu'en soit la forme (papier, électronique, numérique, orale, …) utilisés par Cluster Défense Sécurité pour assurer les formations, demeurent la propriété exclusive de Cluster Défense Sécurité. À ce titre ils ne peuvent faire l'objet d'aucune utilisation, transformation, reproduction, exploitation non expressément autorisée au sein ou à l'extérieur du Client sans accord exprès de Cluster Défense Sécurité. En particulier, le Client s'interdit d'utiliser le contenu des formations pour former d'autres personnes que son propre personnel et engage sa responsabilité sur le fondement des articles L. 122-4 et L. 335-2 et suivants du code de la propriété intellectuelle en cas de cession ou de communication des contenus non autorisée. Toute reproduction, représentation, modification, publication, transmission, dénaturation, totale ou partielle des contenus de formations sont strictement interdites, et ce quels que soient le procédé et le support utilisés. Cluster Défense Sécurité demeure propriétaire de ses outils, méthodes et savoir-faire développés antérieurement ou à l'occasion de l'exécution des prestations chez le Client.

5.6. Confidentialité. Les parties s'engagent à garder confidentiels les informations et documents concernant l'autre partie de quelque nature qu'ils soient, économiques, techniques ou commerciaux, auxquels elles pourraient avoir accès au cours de l'exécution du contrat ou à l'occasion des échanges intervenus antérieurement à la conclusion du contrat, notamment l'ensemble des informations figurant dans la proposition commerciale et financière transmise par Cluster Défense Sécurité au Client. Cluster Défense Sécurité s'engage à ne pas communiquer à des tiers autres que ses sociétés affiliées, partenaires ou fournisseurs, les informations transmises par le Client, y compris les informations concernant les Utilisateurs.

5.7. Communication. Le Client accepte d'être cité par Cluster Défense Sécurité comme client de ses offres de services, aux frais de Cluster Défense Sécurité. Sous réserve du respect des dispositions de l'article 6.5, Cluster Défense Sécurité peut mentionner le nom du Client, son logo ainsi qu'une description objective de la nature des prestations, objet du contrat, dans ses listes de références et propositions à l'attention de ses prospects et de sa clientèle notamment sur son site internet, entretiens avec des tiers, communications à son personnel, documents internes de gestion prévisionnelle, rapport annuel aux actionnaires, ainsi qu'en cas de dispositions légales, réglementaires ou comptables l'exigeant.

5.8. Protection des données à caractère personnel. En tant que responsable du traitement du fichier de son personnel, le Client s'engage à informer chaque Utilisateur que :
- des données à caractère personnel le concernant sont collectées et traitées par Cluster Défense Sécurité aux fins de réalisation et de suivi de la formation,
- la connexion, le parcours de formation et le suivi des acquis des Utilisateurs sont des données accessibles à ses services,
- conformément au Règlement général sur la protection des données (RGPD) l'Utilisateur a la possibilité d'exercer son droit à l'effacement (« droit à l'oubli ») en contactant par écrit le cabinet Cluster Défense Sécurité 115 rue Saint-Dominique 75007 Paris,
- le Client est responsable de la conservation et de la confidentialité de toutes les données qui concernent l'Utilisateur et auxquelles il aura eu accès. Cluster Défense Sécurité conservera, pour sa part, les données liées à l'évaluation des acquis par l'Utilisateur, pour une période n'excédant pas la durée nécessaire à l'appréciation de la formation.

5.9. Droit applicable – Attribution de compétence. Les présentes conditions générales sont régies par le droit français. En cas de litige survenant entre le client et Cluster Défense Sécurité à l'occasion de l'exécution du contrat, il sera recherché une solution à l'amiable et, à défaut, le règlement du litige sera du ressort du tribunal de commerce de Paris.

Créé en 2008, le cabinet Cluster Défense Sécurité propose notamment des formations et accompagnements portant sur la sécurité de l'information et la protection des données sensibles. Il s'appuie sur une pédagogie innovante mêlant expertise technique, comportements humains et connaissance du monde de l'entreprise, principalement dans le secteur aéronautique, défense et sécurité (ADS).

Cette approche unique et novatrice permet de proposer des formations et accompagnements à la pointe de l'expertise technique, s'appuyant sur une pédagogie confirmée, tout en répondant à vos besoins d'une manière la plus opérationnelle possible. Pour compléter ces formations, nous offrons aux stagiaires la possibilité de rejoindre un espace d'échanges (bonnes pratiques, ressources documentaires…) sur Citadel Team®. Développée par Thales, Citadel Team® est une plateforme qui permet de rassembler des communautés de professionnels pour échanger des données sensibles, tout en garantissant l'identité des différents interlocuteurs, la protection et la localisation des données.

Notre cabinet fait notamment appel à trois intervenants confirmés ayant chacun une très large expertise, parfaitement complémentaire.

Jean-Michel Back		Saint-Cyrien, breveté de l'Ecole de Guerre, Jean-Michel Back a été responsable de l'ensemble de la politique de protection du ministère des Armées et, en tant que fonctionnaire de sécurité et de défense (FSD), l'un des principaux contributeurs de la rédaction de la nouvelle réglementation sur la protection du secret de la défense nationale. Il est par ailleurs « expert en intelligence économique et protection des entreprises » (INHESJ).
Pascaline Abdini		Pascaline Abdini est spécialisée dans les projets novateurs et complexes dans les domaines RH et utilise une pédagogie qui favorise l'intelligence collective et l'implication des collaborateurs. Elle est à l'origine de Data Shield, un dispositif innovant destiné à aligner les comportements humains sur la politique de protection des données des organisations. Elle est certifiée « coach professionnelle » « maître praticien PNL » « consultante Investigation Appreciative » et « sécurité économique et protection du patrimoine » (IHEDN).
Patrice Lefort-Lavauzelle		Patrice Lefort-Lavauzelle est spécialisé dans l'accompagnement des entreprises technologiques en France et à l'international, notamment dans le domaine de la protection de l'information. Il est également impliqué au niveau régalien dans différents sujets concernant la protection physique, la cyber-sécurité, la protection du secret de la défense nationale, ainsi que la protection du potentiel scientifique et technique de la nation (PPST) et a publié de nombreux articles sur ces sujets. Il est certifié « officier de sécurité » et « officier de sécurité des systèmes d'informations » au niveau « Expert ».

Quelques exemples d'articles et d'interviews :

- *La réforme du secret de la défense nationale* (Patrice Lefort-Lavauzelle) (Portail de l'IE).
- *Les collaborateurs au centre de la protection des données* (Pascaline Abdini) (revue S&D Magazine, numéro spécial FIC 2020).
- Interview de Pascaline Abdini sur le programme Data Shield® dans le Livre blanc d'Ercom « *Protection des données : pourquoi et comment RSSI et DSI doivent-ils collaborer ?* ».
- *Partager les outils de lutte contre la cybermalveillance*. Entretien avec Jérôme Notin, directeur général du dispositif d'assistance aux victimes de cybermalveillance (Patrice Lefort-Lavauzelle) (revue Défense, Union-IHEDN).
- *Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) : outil de lutte contre l'espionnage technologique* (Patrice Lefort-Lavauzelle) (Sécurité & Stratégie, revue des directeurs de sécurité d'entreprise) (CDSE).
- *La cryptographie quantique ou la distribution quantique des clefs* (Patrice Lefort-Lavauzelle) (revue Défense, Union-IHEDN).

Le cabinet Cluster Défense Sécurité est un organisme de formation
enregistré sous le numéro 11 75 45983 75 auprès du préfet de région d'Ile de France.

Datadock

Organisme validé et référencé

Les formations et une partie des accompagnements proposés par le cabinet Cluster Défense Sécurité sont éventuellement éligibles à votre plan de formation.

Pascaline Abdini et son équipe pédagogique sont à votre disposition pour répondre à vos questions.

www.clusterdefensesecurite.fr

www.datashield.fr

Cluster Défense Sécurité, 115 rue Saint-Dominique 75007 Paris
SAS au capital de 5.000 euros. RCS Paris : B 522 942 424