

ANNEXE 1 au contrat

Obligations en matière de protection des données et de sécurité

Conformément à l'article ~~7.4.VII.6.1~~ 7.4.VII.6.1.2 du Contrat, le Titulaire met en œuvre les mesures techniques et organisationnelles suivantes :

Sujet	Mesure de sécurité	Niveaux de maturité
Gestion des habilitations des utilisateurs des applications fournies par France Travail en cohérence avec l'activité réalisée	L'organisme de formation titulaire doit s'assurer régulièrement que les habilitations des utilisateurs des applications fournies par France Travail sont en cohérence avec l'activité qu'ils réalisent.	<p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>réalisée tous les 3 mois, avec un</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>(PV) établi et transmis à France Travail. Les habilitations sont, quant à elles, traitées au fil de l'eau.</p>
		<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>avec PV réalisé et transmis à FT</p>
		<p>Non conforme</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>a mis en forme : Justifié, Espace Après : 0 pt</p>
		<p>a mis en forme : Espace Après : 0 pt</p> <p>formation dispose d'une procédure, fournit la</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>l'applique en cas d'incident</p>
Procédure en cas d'incidents	L'organisme de formation titulaire doit avoir une procédure et communiquer tout incidents affectant les données fournies par France Travail dans les 48 heures après avoir pris connaissance de l'incident. Réf clause RGPD : VII.3.1.4 - <i>Violation de données personnelles</i>	<p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>formation ne dispose d'aucune procédure ou n'applique pas la</p>
		<p>Non conforme</p>

		procédure existante	
Sécurisation des échanges entre le Titulaire et tout intervenant prenant part à l'exécution du marché	L'organisme doit mettre en œuvre un moyen sécurisé et conforme au RGPD pour assurer les échanges entre lui-même et les différents formateurs, notamment les indépendants.	<p>Avancé</p> <p>fichiers chiffrés par un outil qualifié par l'ANSSI (Primxzed! par ex.) ou mise à disposition des fichiers sur un portail avec deux facteurs.</p>	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		<p>Intermédiaire</p> <p>email, utilisation d'un système d'information (propre ou externalisé)</p>	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		<p>Basique / Minimal</p> <p>fichier chiffré par outil de chiffrement standard.</p>	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		Non conforme	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
Stockage des données	Il est interdit d'utiliser les offres publiques des plateformes de stockage non maîtrisée (Google Drive, Dropbox, etc.) pour y transférer les données transmises par France Travail. Cette mesure est également applicable aux formateurs.	<p>Basique / Minimal</p> <p>plateforme de ce type utilisée</p>	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		Non conforme	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		stockage non maîtrisée	

<p>Destruction des données personnelles</p>	<p>L'organisme de formation doit régulièrement détruire les données obtenues il y a plus de 6 mois. Il doit fournir un procès-verbal de destruction.</p> <p>Réf clause RGPD : VII.3.1.5 - Sort des données</p> <p>Cette mesure est également applicable aux formateurs.</p>	<p>Basique / Minimal</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>destruction transmis à France Travail tous les 6</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p>	
		<p>Non conforme</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p>	
		<p>Non conforme</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p>	
<p>Condition de détention du matériel informatique dans des locaux appropriés et sécurisés</p>	<p>L'organisme de formation doit héberger le matériel informatique dans des locaux appropriés et sécurisés.</p>	<p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>les serveurs soutenant la messagerie les espaces de</p> <p>Avancé</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>et l'AD.</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>Intermédiaire</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>d'accès</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>Basique / Minimal</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>contrôle d'accès</p> <p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>Non conforme</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>simple ou</p> <p>Armure</p> <p>technique sans</p> <p>cônetre d'accès</p>	

Utilisation de messageries électroniques accessibles via Internet	<p>En cas d'utilisation de messageries électronique accessible via Internet, par exemple par un <i>webmail</i>, l'organisme de formation doit disposer d'une authentification sécurisée à ce service.</p> <p>Cette mesure est également applicable aux formateurs.</p>	Avancé	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>2FA sur deux supports différents</p>
		Basique / Minimal	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>de passe robuste</p>
			<p>a mis en forme : Centré, Espace Après : 0 pt</p>
			<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>protection contre les attaques par force brute</p>
			<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>mot de passe qui ne transfère pas le mot de passe mais laisse la possibilité unique à l'utilisateur de le choisir.</p>
		Non conforme	<p>a mis en forme : Centré, Espace Après : 0 pt</p> <p>a mis en forme : Justifié, Espace Après : 0 pt</p>
Utilisation d'application, de service de partage de fichiers, etc. accessible via Internet	<p>En cas d'utilisation d'application, de service de partage de fichiers, etc. accessible via Internet, l'organisme de formation doit disposer d'une authentification sécurisée à ce service.</p> <p>Cette mesure est également applicable aux formateurs.</p>	Avancé	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>multi facteurs reposant sur l'association de plusieurs facteurs d'authentification appartenant à une catégorie de facteurs différente parmi les facteurs de connaissance, de</p>
			<p>a mis en forme : Centré, Espace Après : 0 pt</p>

		possession et inhérent	
		de passe robuste	a mis en forme : Justifié, Espace Après : 0 pt
		protection contre les attaques par force brute	a mis en forme : Justifié, Espace Après : 0 pt
		Basique Minimal	a mis en forme : Centré, Espace Après : 0 pt
		d'oubli de mot de passe qui ne transfère pas le mot de passe mais laisse la possibilité unique à l'utilisateur de le choisir.	a mis en forme : Justifié, Espace Après : 0 pt
		Non conforme	a mis en forme : Centré, Espace Après : 0 pt
Configuration du Wifi	L'organisme de formation doit mettre en place une configuration du WiFi à l'état de l'art. https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_WIFI_NoteTech.pdf	Avancé	a mis en forme : Justifié, Espace Après : 0 pt
		la diffusion SSID + WPA2	a mis en forme : Centré, Espace Après : 0 pt
		point d'accès	a mis en forme : Justifié, Espace Après : 0 pt
		Basique Minimal pour utiliser un chiffrement robuste.	a mis en forme : Centré, Espace Après : 0 pt

		Utilisation du mode WPA2 avec l'algorithme de chiffrement AES-CCMP.	
		Non conforme	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
Moyens de protection de la connexion et navigation sur Internet	L'organisme de formation doit mettre en œuvre des moyens de protection depuis Internet et de la navigation web.	Avancé	<p>a mis en forme : Justifié, Espace Après : 0 pt</p>
		Basique	a mis en forme : Centré, Espace Après : 0 pt
		Minimal	a mis en forme : Justifié, Espace Après : 0 pt
		Non conforme	a mis en forme : Centré, Espace Après : 0 pt
		Non conforme	a mis en forme : Justifié, Espace Après : 0 pt
		Non conforme	a mis en forme : Centré, Espace Après : 0 pt
Connaissance par le Titulaire de son système d'information	L'organisme de formation doit disposer de la connaissance de son système d'information	Non conforme	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		Basique	a mis en forme : Centré, Espace Après : 0 pt
		Minimal	a mis en forme : Justifié, Espace Après : 0 pt
Protection de tous les terminaux	L'organisme de formation doit disposer de moyen de protection des terminaux utilisés. Cette mesure est également applicable aux formateurs.	Avancé	a mis en forme : Justifié, Espace Après : 0 pt
		Intermédiaire	<p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		Basique	a mis en forme : Centré, Espace Après : 0 pt
		Minimal	<p>a mis en forme le tableau</p> <p>a mis en forme : Justifié, Espace Après : 0 pt</p> <p>a mis en forme : Centré, Espace Après : 0 pt</p>
		Non conforme	a mis en forme : Justifié, Espace Après : 0 pt
		Non conforme	a mis en forme : Centré, Espace Après : 0 pt
		Non conforme	(BYOD) sans inscription MDM/EMM, sans

		chiffrement et sans contrôle d'accès.	
Formation et sensibilisation du personnel aux bonnes pratiques de sécurité des systèmes d'information (SSI).	L'organisme doit sensibilisé et former son personnel aux bonne pratiques SSI	Non conforme	<p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>programme de sensibilisation n'est en place. Le personnel n'a pas conscience des risques liés à la cybersécurité, ce qui expose l'organisation à</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>importantes.</p>
		Basique / Minimal	<p>← a mis en forme : Espace Après : 0 pt</p> <p>intervenant dans le cadre de la démarche est formé et sensibilisé aux risques liés à la cybersécurité.</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p>
		Avancé	<p>← a mis en forme : Justifié, Espace Après : 0 pt</p> <p>de sensibilisation est formalisé et diffusé</p> <p>← a mis en forme : Centré, Espace Après : 0 pt</p> <p>l'ensemble du personnel. La démarche est proactive.</p>

Gouvernance des nouvelles technologies (IA)

L'organisme doit encadrer l'usage de l'IA pour éviter les risques de sécurité, de confidentialité et de dérives.

Non conforme	n'est pas encadré. Les collaborateurs peuvent utiliser librement des outils d'IA sans directives ni sensibilisation aux risques, notamment en matière de cybersécurité.	a mis en forme : Justifié, Espace Après : 0 pt
Basique Minimal	encadré par une politique	a mis en forme : Justifié, Espace Après : 0 pt
	à la gouvernance	a mis en forme : Centré, Espace Après : 0 pt
	de sensibilisation sont menées.	a mis en forme : Centré, Espace Après : 0 pt
Avancé	encadré par une politique claire, intégrée à la gouvernance SSI. Les contenus sont régulièrement mis à jour, des campagnes de sensibilisation	a mis en forme : Justifié, Espace Après : 0 pt
	créées sont menées, et des référents accompagnent les utilisateurs. L'usage est audité et les risques sont évalués de manière proactive.	a mis en forme : Centré, Espace Après : 0 pt

Dès la notification du marché, le Titulaire est tenu de mettre en œuvre, *a minima*, l'ensemble des mesures minimales définies.

Six mois après la date de notification du marché, le Titulaire rend compte à France Travail de cette mise en œuvre en lui retournant, au format Excel, le questionnaire Cybersécurité remis lors de la réunion de lancement. Ce questionnaire permet de définir le type de mesures effectivement mises en œuvre (minimal, intermédiaire, avancé).

Un plan de progrès pourra être demandé suivant les résultats issus du questionnaire.