ANNEXE 1 – OBLIGATION EN MATIERE DE PROTECTION DES DONNEES ET DE SECURITE

Conformément à l'article 6.4 du Contrat, le Titulaire met en œuvre les mesures techniques et organisationnelles suivantes :

Processus à sécuriser	Mesures à mettre en œuvre	Niveaux d'exigence
Gestion des habilitations des utilisateurs des applications fournies par France Travail en cohérence avec l'activité réalisée	La vérification des habilitations doit être effectuée par le Titulaire tous les 6 mois.	Minimal
	Le Titulaire établit un procès-verbal de cette revue d'habilitation et le transmet à France Travail.	Avancé
Sécurisation des échanges entre le Titulaire et tout intervenant prenant part à l'exécution du marché	Les échanges s'effectuent par envoi par courriel de fichiers chiffrés avec un outil standard type 7zip.	Minimal
	Les échanges s'effectuent par envoi par courriel de fichiers chiffrés avec un outil qualifié par l'ANSSI (Primx zed! par exemple) ou par la mise à disposition de fichiers sur un portail avec authentification à deux facteurs.	Avancé
Stockage des données	Le Titulaire interdit à l'ensemble des intervenants prenant part à l'exécution du marché d'utiliser les offres publiques des plateformes de stockage non maîtrisées pour y transférer les données transmises par France Travail.	Minimal
Destruction des données personnelles	Le Titulaire réalise une purge tous les 6 mois de l'ensemble des données qui ne sont plus nécessaires à l'exécution du marché.	Minimal
	Le Titulaire réalise une purge tous les 6 mois de l'ensemble des données qui ne sont plus nécessaires à l'exécution du marché. Il établit un procès-verbal de destruction qu'il transmet à France Travail.	Avancé
Condition de détention du matériel informatique dans des locaux appropriés et sécurisés	Le Titulaire conserve le matériel informatique dans une armoire technique.	Minimal
	Le Titulaire conserve le matériel informatique dans une salle technique avec contrôle d'accès.	Intermédiaire
	Le Titulaire conserve le matériel informatique dans un centre de données pour les serveurs soutenant la messagerie, les espaces de stockage partagé et l'Assistance Diagnostic.	Avancé
Utilisation de messageries électroniques accessibles via Internet	Le Titulaire met en œuvre : • une politique de mot de passe robuste (mot de passe de 8 caractères dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial ou mot de passe de plus de 12 caractères) ; • un mécanisme de protection contre les attaques par force brute (par exemple : temporisation d'accès au compte après plusieurs échecs ; nombre maximal de tentatives autorisées dans un délai donné ; mise en place d'un "Captcha" ; blocage du compte après 10 échecs assorti d'un mécanisme de déblocage choisi	Minimal

	en fonction des risques d'usurpation d'identité et d'attaques ciblées par déni de service) ; • un mécanisme d'oubli de mot de passe qui ne transfère pas le mot de passe mais fourni uniquement à l'utilisateur la possibilité de réinitialiser son mot de passe et donc d'en choisir un nouveau par lui-même.	
	Le Titulaire utilise l'authentification à deux facteurs (2FA) sur deux supports différents.	Avancé
Configuration du Wifi	Le Titulaire 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 avec un mode d'authentification WPA-PSK avec un mot de passe long (> 20 caractères)	Minimal
	Le Titulaire 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. Il doit configurer le point d'accès pour utiliser un chiffrement robuste (utilisation du mode WPA2 avec l'algorithme de chiffrement AES-CCMP).	Avancé
Moyens de protection de la connexion et navigation sur Internet	Le Titulaire doit disposer d'un pare-feu entrant sur la connexion internet et d'un pare-feu local sur les postes de travail.	Minimal
	Le Titulaire doit disposer d'un proxy web de sortie avec liste de blocage.	Avancé
Connaissance par le Titulaire de son système d'information	Le Titulaire réalise l'inventaire de l'ensemble de ses équipements, services, logiciels, données, traitements de données, accès et interconnexions vers l'extérieur et dispose d'une cartographie à jour de tous les systèmes.	Minimal
Protection de tous les terminaux	Le Titulaire dispose d'antivirus à jour des signatures sur tous les postes de travail.	Minimal
	Des dispositifs de détection et réponses aux terminaux (EDR) sont installés sur les postes de travail.	Intermédiaire
	Le Titulaire maîtrise également l'ensemble de sa flotte mobile via MDM (Mobile Device Management)	Avancé

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.