



EXIGENCES D'HYGIENE CYBER DES S2I

(systèmes industriels d'infrastructure)

Socle minimal relatif aux marchés de travaux

	Exigences	Pénalités ou retenues
1	<p>Le titulaire devra désigner en son sein un point de contact Cyber (POC cyber) pour les besoins de ses prestations ; celui-ci sera garant des obligations contractuelles de cybersécurité de l'entreprise et de ses sous-traitants. Son niveau minimal requis correspond à la formation en ligne de l'ANSSI dite MOOC ("massive on line open course" = cours en ligne), gratuite. Le programme de la formation sera à communiquer à l'ESID pour validation s'il est différent du MOOC de l'ANSSI.</p> <p>Une attestation de désignation du POC cyber devra être fournie dans l'offre par le titulaire ou, au plus tard, avant la notification du marché. En cas de changement de ce POC en cours d'opération, une nouvelle attestation devra être fournie.</p>	Sans objet.
2	<p>Le dossier d'homologation du système industriel fera l'objet d'une mention de protection au minimum de type "Diffusion restreinte", exigeant un poste de travail isolé ou connecté à un réseau interne de niveau DR dans l'entreprise (aucune connexion à internet). Les exigences de l'instruction interministérielle 901 (II 901) devront être appliquées. Le chiffrement de fichiers sera utilisé pour tous les échanges sensibles sur des réseaux non protégés (Internet...). Le logiciel de chiffrement, à la charge de l'entreprise, devra être autorisé par l'ANSSI (ZED par exemple, ou ACID).</p> <p><i>Nota : La solution ACID est à privilégier.</i></p>	Pénalité forfaitaire de 500 € HT à chaque manquement.
3	<p>Toute personne intervenant sur les systèmes industriels, pour leur conception, mise en place, configuration et maintenance, devra être formée à la cybersécurité. L'entreprise devra pouvoir attester que ces personnes ont suivi une formation ou une sensibilisation aux risques cyber. Le titulaire peut se baser sur les supports et présentations de l'ANSSI pour établir sa formation de sensibilisation ; celle-ci sera à communiquer à l'ESID pour validation.</p>	Pénalité forfaitaire de 1000 € HT à chaque manquement.
4	<p>Tout personnel devant intervenir sur les systèmes devra y avoir été formellement autorisé préalablement par l'ESID, sur un document écrit. A cette fin, le titulaire devra établir la liste des personnes qu'il estime devoir travailler sur les systèmes, en conception, mise en place, configuration ou maintenance.</p>	Pénalité forfaitaire de 300 € HT à chaque manquement.
5	<p>Le prestataire devra établir :</p> <ul style="list-style-type: none"> - la cartographie physique du système industriel qui correspond à la répartition physique des équipements ; - la cartographie des applications (programmes automates, applications de supervision ...). <p>Une cartographie "Projet" sera soumise au stade VISA avant réalisation, et la cartographie finale sera fournie au stade des OPR (opérations préalables à la réception).</p> <p><i>Nota : pour les établir, le titulaire se basera sur les documents de l'ANSSI : "Cartographie du système d'informations" et l'annexe A des "Mesures détaillées".</i></p>	<p>Retenue de 2000 € HT pour le livrable « PROJET ». Cette retenue sera opérée sur le premier décompte mensuel.</p> <p>Retenue de 2000 € HT pour le livrable « FINAL ». Cette retenue sera opérée sur le dernier décompte mensuel.</p> <p>Elles seront appliquées sans mise en demeure préalable et seront payées après la remise complète du livrable.</p>

6	Les postes de travail, les serveurs... devront être installés dans des locaux à accès limité (fermés à clé, ou digicode, ou mobiliers sécurisés ...). L'accès aux équipements du système devra être protégé physiquement : armoires fermées à clé, mise en place de scellés...	Sans objet.
7	L'ensemble des composants installés devra respecter le guide des <i>"Mesures détaillées pour la cybersécurité des systèmes industriels"</i> de l'ANSSI. Les exigences doivent être adaptées à chaque composant. Des exigences complémentaires pourront être transmises à la notification du marché au titulaire.	Pénalité forfaitaire de 500 € HT à chaque manquement.
8	Les postes de supervision et des équipements de terrain (automates) ne devront pas avoir d'accès possible à Internet. L'accès aux ports ethernet et USB du système, ainsi que les connexions sans fil (Wi-Fi, bluetooth, NFC, etc.), seront bloqués si ces derniers ne sont pas utilisés. Les équipements autorisés à se connecter aux installations dans le cadre des interventions devront être clairement identifiés et validés (PC dédiés validés par le bureau SSI de l'ESID) ; ils devront être marqués par le bureau SSI de l'ESID. Une attestation de contrôle cyber de l'équipement devra être en permanence présentable à l'Administration, et présente avec l'équipement.	Pénalité forfaitaire de 500 € HT à chaque manquement.
9	Seuls les médias amovibles (clef USB, disques durs, carte SD...) dédiés au système industriel (c'est-à-dire étiquetés comme tels) pourront se connecter sur le système. L'utilisation de ces médias pour tout autre usage est interdite. Réciproquement, l'utilisation de tout autre média est interdite. Les médias amovibles seront fournis par le titulaire. Ils seront préparés par le BSSI-L avant toute utilisation. Ces médias amovibles devront passer par un sas antiviral (ordinateur de l'USID dit "station blanche") avant d'être connecté au système. Si l'accès à un sas antiviral n'est pas possible, le titulaire s'engagera auprès de l'administration à ce que les médias utilisés ont été vérifiés et sont sains.	Pénalité forfaitaire de 1000 € HT à chaque manquement.
10	Lors de la mise en place, les mots de passe par défaut de sortie d'usine devront être modifiables et modifiés. Les mots de passe devront être transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Elle sera stockée dans un lieu sûr. Chaque modification du mot de passe devra être tracée dans un registre tenu par l'Administration. La longueur et la complexité des mots de passe doivent être adaptées à chaque composant. Ces exigences seront transmises durant la période préparatoire au titulaire.	Pénalité forfaitaire de 500 € HT à chaque manquement.
11	Un processus de sauvegarde des données et configurations du système industriel devra être défini, mis en œuvre et testé afin de permettre leur restauration en cas d'incident. Les données concernées sont toutes les données nécessaires à la reconstruction de l'installation après un sinistre : les programmes, les fichiers de configuration, les firmwares, les paramètres de procédé (réglages d'asservissement par exemple), etc. Cela peut également concerner des données ayant un aspect réglementaire, comme des exigences de traçabilité. Les configurations devront être sauvegardées avant et après toutes modifications, y compris lorsque celles-ci ont été apportées "à chaud". Les sauvegardes seront fournies dans un support amovible (clé USB) sain (c'est-à-dire contrôlé préalablement sur une station antivirale). Le titulaire devra décrire ce processus de restauration des sauvegardes dans une version "Projet", qui sera soumise au stade VISA avant réalisation, puis la version « Finale » sera fournie au stade des OPR (opérations préalables à la réception). Au stade OPR, un test de restauration sera réalisé en présence de la maîtrise d'œuvre.	Retenue de 2000 € HT pour le livrable « PROJET ». Cette retenue sera opérée sur le premier décompte mensuel. Retenue de 2000 € HT pour le livrable « FINAL ». Cette retenue sera opérée sur le dernier décompte mensuel. Elles seront appliquées sans mise en demeure préalable et seront payées après la remise complète du livrable.